SPRING23
+19TH GCPS
A Joint AIChE and CCPS Meeting

Use of Human Reliability Analysis to Supplement LOPA for Scenarios Dominated by Human Error

William Bridges
Process Improvement Institute, Inc.
Knoxville, Tennessee, USA
wbridges@piii.com

Art Dowell, III
Process Improvement Institute, Inc.
Houston, Texas, USA
adowell@piii.com

Matias Massello
Process Improvement Institute, Inc.
La Plata, ARG
mmassello@piii.com

PROCESS IMPROVEMENT INSTITUTE
Risk and reliability specialists

Prepared for Presentation at
American Institute of Chemical Engineers
2023 Spring Meeting and 19th Global Congress on Process Safety
Houston, TX
March 12-16, 2023

AIChE shall not be responsible for statements or opinions contained in papers or printed in its publications

PROCESS IMPROVEMENT INSTITUTE
Risk and reliability specialists

SPRING23
+19TH GCPS
A Joint AIChE and CCPS Meeting

USE OF HUMAN RELIABILITY ANALYSIS TO SUPPLEMENT LOPA FOR SCENARIOS DOMINATED BY HUMAN ERROR

Main authors

William Bridges – President
Process Improvement Institute, Inc. (PII)
e-mail: wbridges@piii.com

Art Dowell, III – Principal engineer
Process Improvement Institute, Inc. (PII)
e-mail: adowell@piii.com

Matías Massello – Process Safety Engineer
Process Improvement Institute, Inc. (PII)
e-mail: mmassello@piii.com

Abstract

There are many scenarios and situations for which Layers of Protection Analysis (LOPA) may not be a suitable methodology or may be difficult to use. One such case is a scenario is dominated by human error and yet there does not appear to be a way to have one or more IPLs. This paper illustrates Human Reliability Analysis ([HRA], including Human Reliability Event Tree [HRET]) which can be an alternative and it illustrates how to augment LOPA and SIL Verification calculations for human error probability estimates. Three cases are covered in this paper:

- HRA used for the risk assessment of the re-built Phillips Polyethylene Plants (Pasadena, TX) following the explosion in 1989 that caused 23 worker fatalities. This occurred during on-line maintenance to clear a large product discharge line. This HRET was required as part of the settlement between Phillips and the US Government.
- Risk assessment of a task at a copper smelter that was addressed using LOPA, while incorporating human-error-prevention IPLs that perhaps other sites have not considered. A list of human error prevention IPLs is shared in the paper.
- HRET used to augment SIL verification to account for the human error appropriately (SIF standards and ANSI/ISA Technical Reports that govern how to do SIL Verification do not include these large human error probabilities.)

This paper will help the implementor understand how to get the most from LOPA in high human error scenarios and when it is appropriate to consider an alternative approach.

Introduction

Human error can be an initiating event of a scenario or humans can serve as an Independent Protection Layer (IPL) in response to a critical alarm or other call for action. Rules of LOPA do not allow counting a human more than once in the same scenario. Instead, the owners of the process try to find IPLs that are unrelated to the human action that is the initiating event or other IPL. But in some cases, the owners want to see if it is appropriate to use a human more than one. Human reliability analysis methods have been used since the late 1960 do so just that.

Why do some look beyond LOPA?

LOPA is a valuable risk assessment method as demonstrated by its extensive use for the past 28 years. It is relatively easy for technical staff to learn and adds clarity to risk assessment of the more complex accident scenarios. What makes LOPA particularly useful are the rigid rules used in LOPA. The same rules limit the flexibility of LOPA. The result is that for scenarios that are very complex, such as where components are shared to some extent or where humans serve in protective functions more than once, LOPA cannot normally be used. This is a limitation that the inventors of the LOPA rules were aware of; but that was not a major concern 28 years ago or today because there are alternative methods for handling scenarios that do not fit within the usefulness of LOPA.

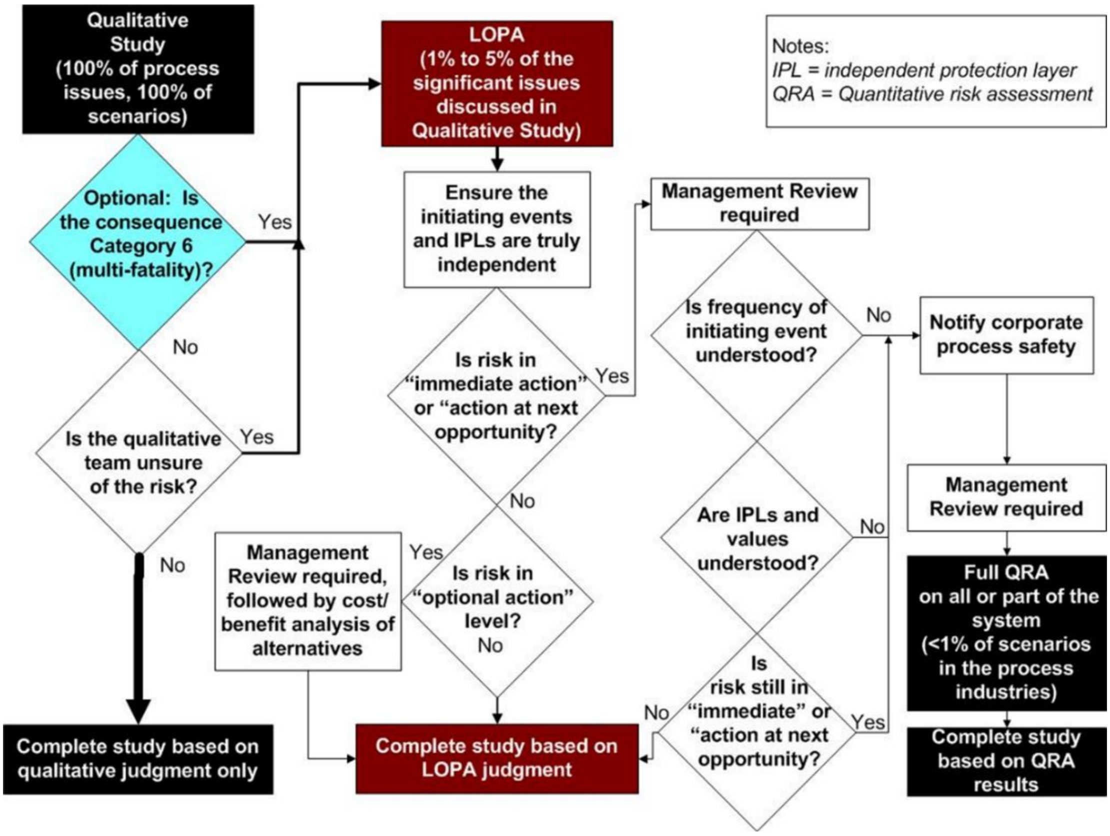

Qualitative Study (100% of process issues, 100% of scenarios)
Optional: Is the consequence Category 6 (multi-fatality)?
Yes
No
Is the qualitative team unsure of the risk?
Yes
No
Complete study based on qualitative judgment only
LOPA (1% to 5% of the significant issues discussed in Qualitative Study)
Ensure the initiating events and IPLs are truly independent
Is risk in "immediate action" or "action at next opportunity?
Yes
No
Is risk in "optional action" level?
Yes
No
Management Review required, followed by cost/ benefit analysis of alternatives
Complete study based on LOPA judgment
Notes:
IPL = independent protection layer
QRA = Quantitative risk assessment
Management Review required
Is frequency of initiating event understood?
No
Are IPLs and values understood?
No
Is risk still in "immediate" or "action at next opportunity?
No
Yes
Notify corporate process safety
Management Review required
Full QRA on all or part of the system (<1% of scenarios in the process industries)
Complete study based on QRA results

Figure 1. When to Use LOPA and When to Use QRA/HRA

Quantitative Risk Assessment (QRA) methods are a set of alternative tools that have been used since the late 1960s and include Human Reliability Analysis (HRA) that was originally developed for assessing the risk of nuclear power reactors. These methods were pioneered by Dr. Alan Swain.

HRA Overview

HRA is a collection of methods and techniques that are available for predicting human error. In a review of human reliability assessment methods, the UK HSE identified a total of 72 potential human reliability tools and acronyms, 35 of which were fully investigated [1]. Some of the techniques are:

- THERP (Technique for Human Error Rate Prediction).
- HEART (Human Error Assessment and Reduction Technique).
- SLIM (Success Likelihood Method).
- HCR (Human Cognitive Reliability).
- APJ (Absolute Probability Judgment)

In carrying out an HRA, it is necessary to identify those human actions that can influence system reliability or availability. The most common application of HRA is the evaluation of human acts required in a system context. The consideration of extraneous actions is also important. The person in a system may not only fail to do what he is supposed to do, or fail to do it correctly, but he may also do something extraneous that could degrade the system. The latter is the weak link in HRA. It is not possible to anticipate all undesirable extraneous human actions. The best anyone can do is to identify those actions having the greatest potential for degrading system reliability and availability. The assignment of probability estimates to extraneous actions is difficult and uncertain. Often the best one can do is to estimate very broad ranges of probabilities of human errors that one believes include the true probability. Fortunately, the probabilities of extraneous actions are usually very low. [2]

The quantified HRA methods typically require significant training and experience before an analyst is proficient in their use. More recently, effort has been applied to develop simplified tools to be used either in PHAs, LOPAs or with slight extensions of LOPA. These include:

- **PHA Team qualitative judgement:** This is the simplest method. It relies completely on the experience and judgment of the PHA Team. Team members usually use the aid of the qualitative descriptions in a Risk Matrix. This method requires that at least one of the members is knowledgeable in Human Reliability and Human factors. Due to the simplicity of the method, the uncertainty can be significant and therefore it does not work properly for complex scenarios, scenarios with high consequences, or scenarios dominated by Human Error.
- **LOPA limit rule for IEF:** LOPA provides a bridge between Qualitative analysis and Quantitative analysis. It has a simple set of rules, which usually are conservative to compensate with the simplicity and ease-of-use of the rules. Within those rules, there is one that limits the probability of a Human Error (HEP): for a task that is performed several times a year (high practice); the lowest value that can be used is 1 (per year). That value assumes good control of Human Factors.

- **LOTO lower limit rule:** Another LOPA rule, related to the previous bullet, applies to the Lock-Out-Tag-Out procedures that are usually mentioned as safeguards in scenarios that involve human errors. Assuming good control of Human Factors, the lowest PFD value for the Human IPL of the LOTO procedure is 1 in 1000 (1E-3).

Human Reliability Event Tree (HRET) overview

A common HRA tool for complex human actions is the HRA event tree, which is associated with the THERP method cited above. It incorporates a pyramid of branches representing human success and failure paths. The branches terminate at a point when the task is successfully completed or when an unrecoverable error (leading to a system failure) occurs. The tree can be solved mathematically using conditional probability, where the probability of the successful completion of a task or step depends on the success or failure of the previous step or task. This is represented in Figure 2 below:

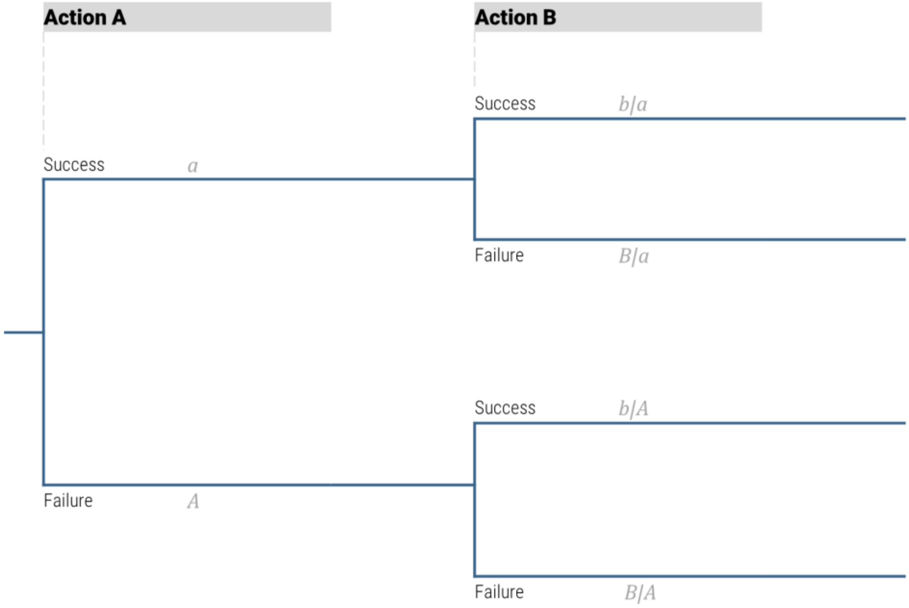


Figure 2. Human Reliability Analysis (HRA) Tree logic

Where:

- a = probability of the successful performance of Action A
- A = probability of the unsuccessful performance of Action A
- b|a = probability of the successful performance of Action B, given a
- B|a = probability of the unsuccessful performance of Action B, given a
- b|A probability of the successful performance of Action B, given A
- B|A = probability of the unsuccessful performance of Action B, given A

By definition the following conditions are met:

$$P[Success] + P[Failure] = P[a] + P[A] = P[b] + P[B] = 1 \qquad \text{[Eq. 1]}$$

As an example, for a series system in which Action B is performed after Action A and both tasks have to be performed correctly in order to get the desirable output, the calculations are:

$$P[S] = a \times (b|a) \qquad \text{[Eq. 2]}$$

$$P[F] = 1 - P[S] = 1 - a \times (b|a) \qquad \text{[Eq. 3]}$$

In cases where the possibility of detecting and fixing a mistake in either Action, the Event Tree shown in Figure 2, gets slightly modified (Figure 3).

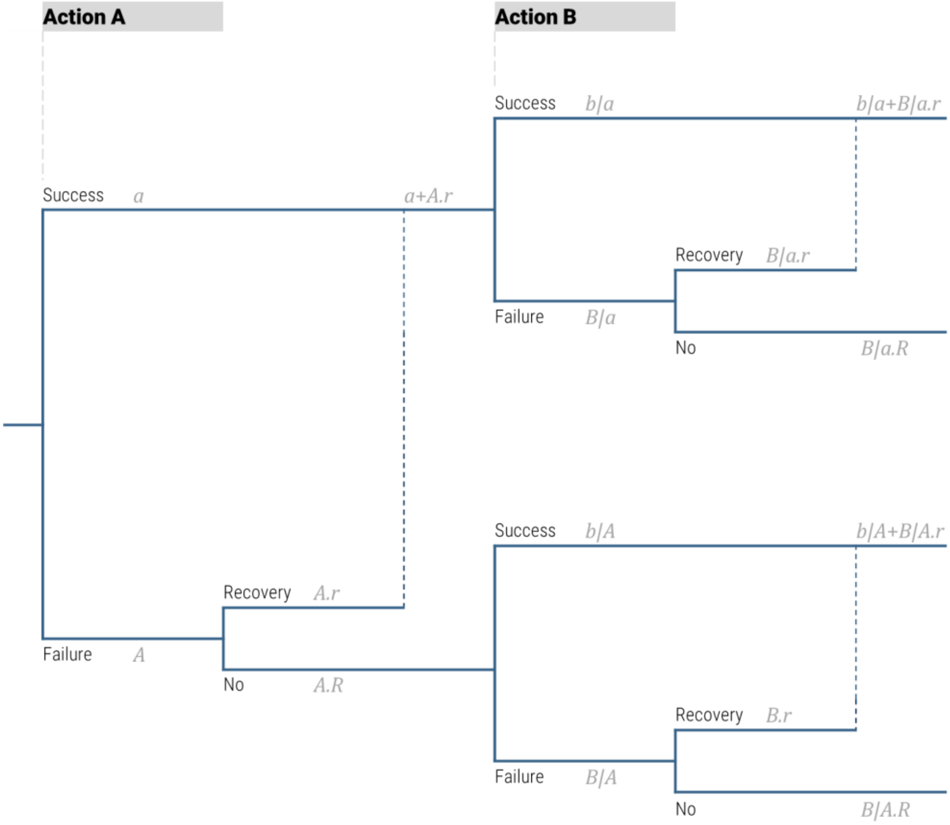


Figure 3. Human Reliability Analysis (HRA) Tree logic with Recovery

Where:

- r = recovery (i.e., Fraction of times in which a Failure is detected and corrected before performing Action B)
- R = non-recovery (i.e., Fraction of times in which a Failure remains undetected and it is not corrected before performing Action B)

Considering recovery, the 2oo2 example shown in [Eq. 2] and [Eq. 3] is now calculated as:

$$P[S] = (a + A \times R) \times [(b|a) + (B|a) \times r] \qquad \text{[Eq. 4]}$$

$$P[F] = 1 - P[S] = 1 - (a + A \times R) \times [(b|a) + (B|a) \times r] \qquad \text{[Eq. 5]}$$

Overview of Human Error probabilities and dependency

Human Error Probability for a Single Execution of a Rule-Based Task

To calculate P_{HUMi}, the type of tasks must be defined and the baseline error rate for such a task must be established. Note that with excellent control of all human factors, a company can begin to approach the lower limits that have been observed for human error, but individual, specific human error probabilities may average about P_{HUMi} = 0.01. It is critical to provide detection and correction for specific human errors.

Excellent control of all human factors requires a robust design and implementation of management systems for each human factor with a high level of operational discipline. The first well-researched publication detailing potential lower limits of human error probability was by Alan Swain and H Guttmann [2] and by others. However, many times, the limits they referenced get used out of context. The lower limits in the NUREG-1278 assume excellent human factors, but such excellent control is rarely, if ever achieved. Additionally, some human errors listed by Swain and others were for a single error under highly controlled conditions, or on a "best day" instead of average error probability or rate over an average year of tasks. In general, Process Improvement Institute (PII) has found it best to use the average error probabilities as discussed in the following section.

Error Probability for Rule-Based Actions that are Not Time Dependent:

Actions that do not have to be accomplished in a specific time frame to be effective are not time dependent. It should be obvious then that these do not include response to alarms, or similar actions with time limits. Values listed below represent the lower limits for human error rates, assuming excellent control of human factors; these are expressed as the probability of making a mistake on any step:

- 1/100 - process industry; routine tasks performed 1/week to 1/day. This rate assumes excellent control of all human factors. Most places PII visits, the workers and managers and engineers believe this is achievable, but not yet achieved.
- 1/200 - pilots in the airline industry; routine tasks performed multiple times a day with excellent control of human factors. This average has been measured by a few clients in the airline industry, but for obvious reasons they do not like to report this statistic.
- 1/1000 - for a reflex (hard-wired) action, such as either proactive or minor corrective actions while driving a car, or very selective actions each day (such as simple check and calibrations) where your

job depends on getting it right each time and where there are error recovery paths (such as clear visual cues) to correct the mistake; practice rate is a big factor in getting these low rates; the practice per year needs to be in the range of 500 to 2000 or higher per year.

See Bridges and Collazo [3] for more details on this topic.

Adjusting the lower limit rates to estimate a baseline rate at a site

As mentioned earlier, the lower limit rates assume excellent control of human factors in the industry mentioned. Note that airline pilots have a lower error rate than what PII has measured in the process industry. This is due, in part, to the much tighter control by the airlines and regulators on factors such as fitness-for-duty (control of fatigue, control of substance abuse, etc.). Excellent control of human factors is not achieved in many organizations; therefore, the human error rates will be higher than the lower limit, perhaps much as much as 20 times higher. Table 1 provides adjustment factors for each human factor. These factors can be used to adjust the lower limit of error rate upward or downward as applicable, but the factors should not be applied independently. For instance, even in the worst situations, we have not seen an error rate for an initiating event or initial maintenance error higher than 1/5, although subsequent steps, given an initial error, can have an error rate approaching 1 due to coupling or dependency.

- 1/5 - highest error rates with poor control of human factors; this high rate is typically due to high fatigue or some other physiological or psychological stress (or combination). This is the upper limit of error rates observed with poor human factors and within the process industry. *The error rates in the Isomerization Unit the day of the accident at BP Texas City Refinery were about this rate* [4]. *The operators, maintenance staff and supervisors had been working about 30 days straight (no day off) on 12-hour shifts.*

Table 1. Human factors

Human Factor Category	Human Factor Issue/Level	Multiplier for Cognitive & Diagnosis Errors
Stress/ Stressors (includes staffing issues)	Extreme stress (threat stress; unloading ship with crane non-stop for more than 2 hours, etc.)	5
	High stress (time pressures such as during a maintenance outage; issues at home, etc.)	2
	Nominal	1
Complexity & Task Design	Highly complex task. Or very low complexity/boring task that requires 100% attention for more than 45 min.	5
	Moderately complex (requires more than one staff)	2
	Nominal	1
	Obvious diagnosis	0.2
Experience/ Training* (see the practice rate adjustment in at end of table)	Low experience relative to complexity of task; or poor/no training	10
	Nominal	1
	High	0.5
Procedures	Not available in the field as a reference, but should be. Or 75% accuracy or less ***(normal value for process industry)***	20
	Incomplete; missing this task or these steps; or < 85% accuracy	8
	Available and >90% accurate, but does not follow format rules	3
	Good, 95% accurate, follows >90% of format rules	1
	Diagnostic/symptom oriented	1
Human-Machine Interface (includes tools)	Missing/Misleading (violates populational stereotype; including round valve handle is facing away from worker)	20
	Poor or hard to find the right device; in the head calc	10
	Some unclear labels or displays	2
	Good	1
Fitness for Duty	Unfit (extreme fatigue level at >80 hrs/wk, or >17 hr/day, no day off in 7-day period; or illness, legal intoxicated, etc.)	20
	Highly degraded fitness (high fatigue such as >15 hr/day or >72 hr/wk, or more than 4 consecutive shifts of 12 hours or more; illness, injury, legally barely intoxicated, etc.)	10
	Moderately Degraded Fitness (≥12 hr day or ≥ 60 hours/wk; but at least 1 day off [break] per week)	5
	Slight fatigue (more than 8 hr per day; up to 48 hrs per work week, but at least 1 day off [break] after 48 hours of work ***(normal value for process industry)***	2
	Nominal	1
Work Processes & Supervision	Poor	2
	Nominal	1
	Good	0.8
Work Environment	Extreme (in temp, humidity, noise, lighting, vibration, etc.)	5
	Good	1
Communication	Communication system/interference damaged; poor communication environment	10
	No standard for verbal communication rules ***(normal value for process industry)***	3
	Well implemented and practiced standard	1

Based in part on: Gertman, D.; et. al., The SPAR-H Human Reliability Analysis Method, NUREG/CR-6883, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, August 2005 [5]. PII has modified the list slightly to account for general industry data and terminology and to incorporate PII internal data. *Courtesy Process Improvement Institute, Inc., All Rights Reserved.*

Human Error Probability for Multiple Executions of a Rule-Based Task

Coupled (dependent) Error Rates: Coupling represents the probability of repeating an error (or repeating success) on a second identical task, given that an error was made on the first task. The increased probability of failure on subsequent tasks given that an error has already been made is known as dependence. The list below provides some starting point guidance on values to use:

- 1/20 to1/90 - if the same tasks are separated in time and if visual cues are not present to re-enforce the mistake path. This error rate assumes a baseline error rate of 1/100 to 8/1000 with excellent human factors. If the baseline error is higher, then this rate will increase as well.
- 1/2 - if the same two tasks are performed back-to-back, and if a mistake is made on the first step of two. This error rate assumes a baseline error of 1/100 with excellent human factors. If the baseline error is higher, then this rate will increase as well.
- 8/10 to 10/10 - if the same three tasks are performed back-to-back and a strong visual cue is present (that is, the worker can clearly see the first devices he/she worked on), if a mistake is made on the first steps of the three.
- Two or more people become the same as one person (with respect to counting of errors from the group), if people are working together for more than three days; this effect is due to the trust that can rapidly build.

These factors are based on the relationships provided in NUREG-1278 [2] and the related definitions of weak and strong coupling provided in the training course by Swain (1993) [6] on the same topic, as shown here in Table 2. The following relationship is for errors of omission, such as failing to reopen a root valve or failing to return an SIF to operation, after bypassing the SIF. The qualitative values in Table 2 are based jointly on Swain (1993) and Gertman [5].

One can readily conclude that staggering of maintenance tasks between different maintenance technicians for different channels of the same SIF will greatly reduce the level of dependent errors. Unfortunately, most sites PII visits do not stagger the inspection, test, or calibration of redundant channels of the same SIF or of similar SIFs; the reason they cite is the cost of staggering the staff. While there is a perceived short-term higher cost, the answer may be different when lifecycle costs are analyzed.

Simple Rule: Staggering of maintenance can prevent a significant number of human errors in redundant channels. In fact, the US Federal Aviation Administration (FAA) requires staggering of maintenance for aircraft with multiple engines or multiple control systems (i.e., hydraulics) (FAA Advisory Circular 120-42B, as part of ETOPS approval [7]**.** (ETOPS is Extended-range Twin-engine Operational Performance Standards, a rule which permits twin engine aircraft to fly routes which, at some point, are more than 60 minutes flying time away from the nearest airport suitable for emergency landing).

Table 2. Guideline for Assessing Dependence of Human Actions of Identical or Very Similar Tasks*

Level of dependence	Same person?	Actions close in time?	Same visual frame of reference?	Worker required to write something for each component
Zero (ZD)	No	Yes/No	Yes/No	Yes/No
Zero (ZD)	Yes	No. Separated by several days.	Yes/No	Yes/No
Low (LD)	Yes	Low. Similar tasks performed on sequential days	No	Yes
Moderate (MD)	Yes	Moderate. Similar tasks performed more than 4h apart	No	No
High (HD)	Yes	Yes. Similar tasks are performed within 2h.	No	No
Complete (CD)	Yes	Yes. Similar tasks are performed within 2h.	Yes	Yes/No

* Based partially on SPAR-H, 2005 [17], and partially on field observations by PII. *Courtesy Process Improvement Institute, Inc., All Rights Reserved.*

The level of dependency is determined from Table 2 by assessing whether the same person is doing the tasks, the proximity of the actions in time, the proximity of the actions in space (same visual frame of reference), and whether the work is required to make a record for each component:

1. Read down the “Same Person” column and find the applicable row(s), then.
2. Read down the “Actions Close in Time” column and find the applicable row,
3. Then check the two columns on the right for that row.
4. The Level of Dependence is shown in the left-most column for the applicable row.

Table 2 has two rows for Zero Dependency (ZD) because ZD can be achieved two different ways:

Tasks done by different persons or groups (staggered people), or

Tasks done by same persons or groups, but tasks are done several days apart (staggered times).

Once the level of dependence is known, the probability of either repeat success or repeating errors on identical tasks can be estimated. For these probabilities, we use Table 3, which is a re-typing of Table 20-17 from NUREG-1278 [2] (and the similar table in SPAR-H [5].

Table 3. Equations for conditional probabilities of Success and Failure on Task “N” given Success or Failure on Task “N-1”

Dependence	Success @N given Success @N-1	Failure @N given Failure @N-1
Zero	$P_{Success@N} = 1 - HEP_N$	$P_{Failure@N} = HEP_N$
Low	$P_{Success@N} = [1 + 19 \times (1 - HEP_N)]/20$	$P_{Failure@N} = [1 + 19 \times HEP_N]/20$
Moderate	$P_{Success@N} = [1 + 6 \times (1 - HEP_N)]/7$	$P_{Failure@N} = [1 + 6 \times HEP_N]/7$
High	$P_{Success@N} = [1 + (1 - HEP_N)]/2$	$P_{Failure@N} = [1 + HEP_N]/2$
Complete	$P_{Success@N} = 1$	$P_{Failure@N} = 1$

Case study 01: Phillips disaster (1989)

On the 23rd October 1989, Phillips' 66 chemical complex at Pasadena, near Houston (USA) experienced a chemical release on the polyethylene plant. A flammable vapor cloud formed which subsequently ignited resulting in a massive vapor cloud explosion. Following this initial explosion there was a series of further explosions and fires. The consequences of the explosions resulted in 23 fatalities and between 130 – 300 people were injured. Extensive damage to the plant facilities occurred.

Note that William Bridges, one of the authors of this paper, was the PHA leader in 1991-1992 for the rebuilt polyethylene plants and he was also the analyst for the HRA. The PHA of all modes of operation, including startup, shutdown, and online maintenance and the HRA for the settling leg clearing task were both requirements of the Settlement Agreement between the USA Government and Phillips.

Background

Polyethylene was produced in "loop" reactors (20-in pipes mounted vertically in 150-ft-tall, continuous, ring-like structures) (Figure 5). In the reactor occurs a catalytic reaction at 600 psig (40 barg). Ethylene is the raw feed and liquid isobutane was used as the carrier. Polyethylene "snowflakes" grow in the reactor and settle out as they grow larger and are collected into settling pipes. The polymer fluff is ejected from the settling pipes every few seconds by the opening of small Product Take-Off (PTO) valves (Figure 5 and Figure 6). The polyethylene fluff was expected to move freely through the settling leg, from the loop reactor into the flash tank but in reality, the fluff tended to collect inside the settling legs. Accumulating fluff would develop into a large cylindrical "log" inside the settling leg. Eventually, the log would become large enough to interrupt product transfer between the loop reactor and flash tank.

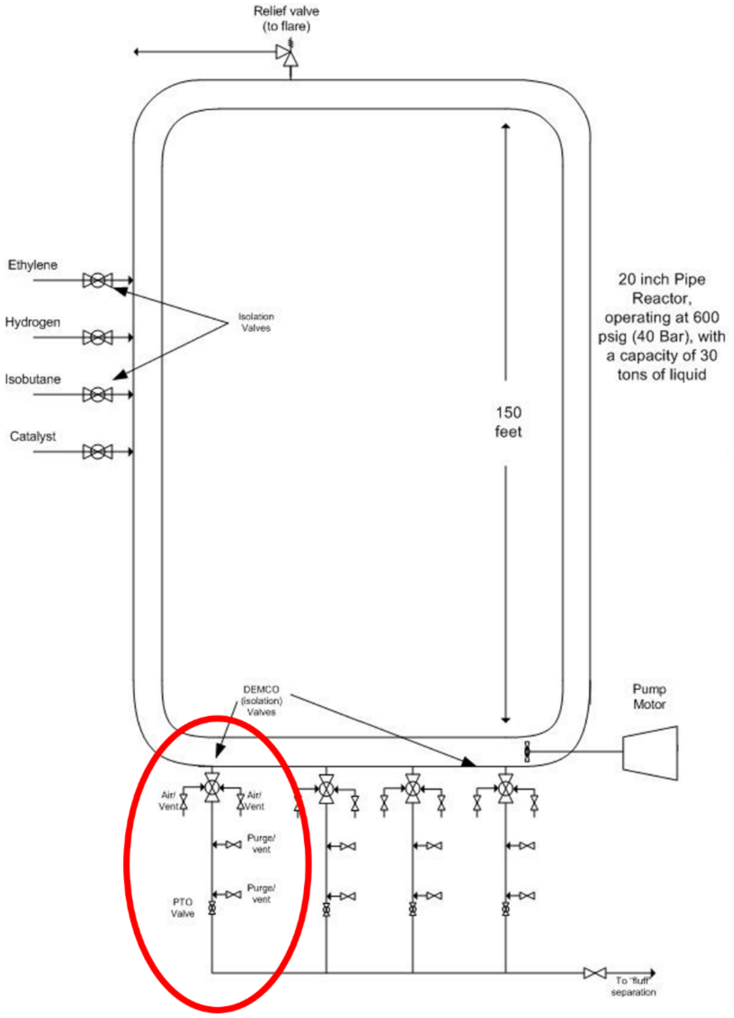
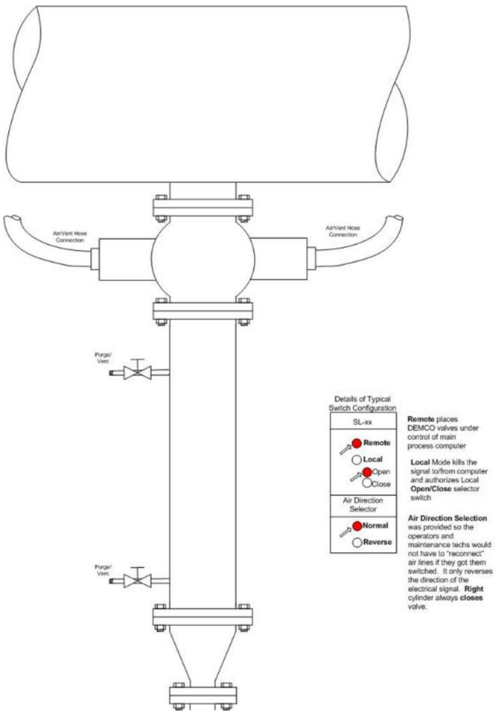


Figure 4. Philips "loop" reactor scheme

Since production would cease if all settling legs became plugged, routine, invasive maintenance was needed to remove the log plugging any of the settling legs. Settling leg maintenance was performed with the loop reactor at normal operating temperature and pressure. Thus, effective energy isolation and control was required before and during settling leg maintenance. Failure to effectively isolate the process could result in the catastrophic loss of flammable reactor contents. Under such circumstances, severe consequences (including multiple fatalities) were possible.



Remote places DEMCO valves under control of main process computer

Local Mode kills the signal to/from computer and authorizes Local **Open/Close** selector switch

Air Direction Selection was provided so the operators and maintenance techs would not have to "reconnect" air lines if they got them switched. It only reverses the direction of the electrical signal. **Right** cylinder always **closes** valve.

Figure 5. "Loop" Reactor settling leg and panel

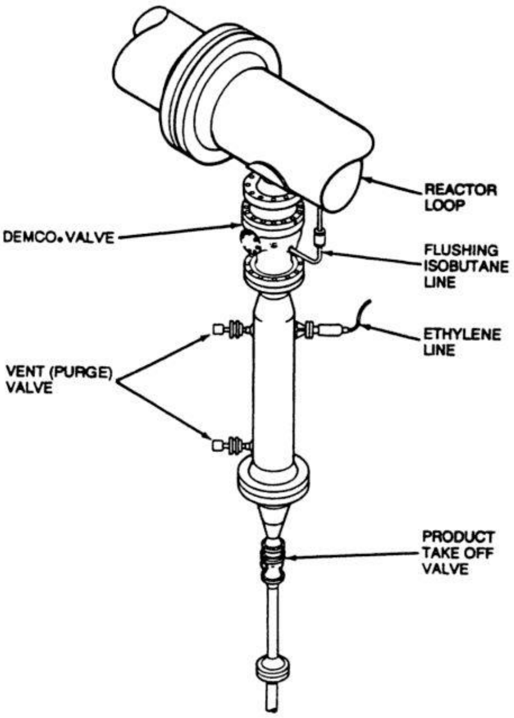


Figure 6. "Loop" Reactor settling leg details

The settling leg unplugging procedure is shown in Table 4 (Note that there was no double-block arrangement, and the procedure is an alternative attempt to provide "double isolation" without inserting a blind flange).

Table 4. Online Maintenance SOP for unplugging settling legs

#	Task	By
1	Close DEMCO in Local mode	Operations
2	Close air and vent lines	Operations
3	Open vent valves on air lines (not shown)	Operations
4	Close PTO valve in local mode (not shown)	Operations
5	Put lock pin into DEMCO valve body (not shown)	Operations
6	Vent settling pipe to flare	Operations
7	Purge settling pipe with nitrogen to air for 1 min	Operations
8	Put operations tags on air cylinder valves, valve body pin, and switches for DEMCO valve and PTO valve	Operations
9	Make sure maintenance begins dismantling/ cleanout promptly	Operations

#	Task	By
10	Check in at control room and make sure which settling pipe to remove	Maintenance
11	Put tags on air cylinder valves, valve body pin, and valve switches	Maintenance
12	Disconnect threaded air hoses from each cylinder of the DEMCO actuator	Maintenance
13	Put pipe cap on end of each air hose	Maintenance
14	Put tag on each pipe cap on end of each air hose	Maintenance
15	Make sure settling pipe is vented to atmosphere and nitrogen purge is turned off	Maintenance
16	Disconnect nitrogen purge line and vent line to flare from settling pipe	Maintenance
17	Hook up chain-hoist from over-head beam to handle on side of settling pipe (not shown)	Maintenance
18	Unbolt and remove settling leg from the 8-inch bottom flange of the DEMCO valve until the 1.5-inch flange above the PTO	Maintenance

**Red steps had not been performed in more than 10 years before the accident for good reasons, but the steps were not deleted from the procedure.*

The average leg plugging frequency was around one per shift per reactor; there are 6 legs per reactor, 8 reactors, and 3 shifts per day. The time required for the unplugging procedure was ~2hr. In some situations, after performing the settling leg unplugging procedure and reopening the DEMCO valve, the leg would "re-plug" with a chunk of plastic that had been stuck inside the cavity of the ball valve. When that situation happened, there is the possibility that the staff may have used an alternative "shortcut" procedure that did not disconnect the air hoses because the settling leg was going to be disconnected for a much shorter period to clear the chunk from the bottom of the setting leg.

Accident description

On the 23rd of October 1989, there was a large release for one of the polyethylene reactors. A flammable vapor cloud formed which subsequently ignited resulting in a massive vapor cloud explosion (Figure 7 and Figure 8). Following this initial explosion there was a series of further explosions and fires.

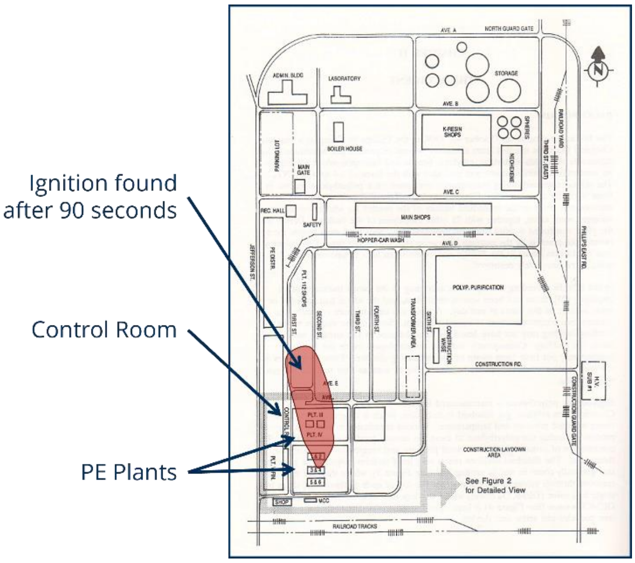


Figure 7. Philips accident release (illustrative only)

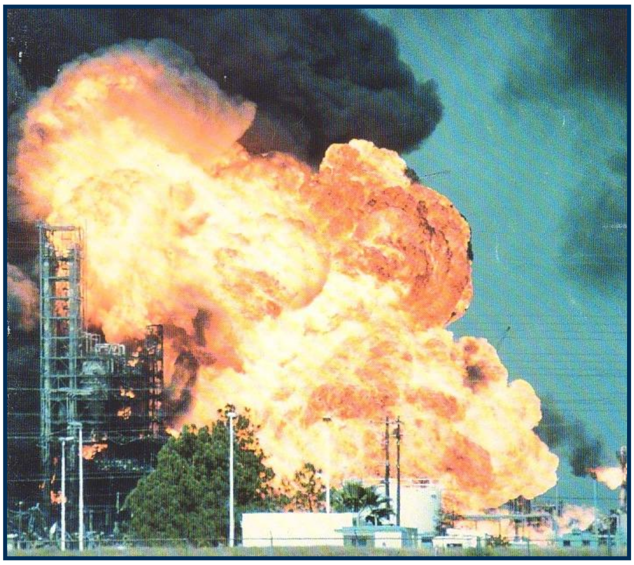


Figure 8. Phillips accident fire

The consequences of the explosions resulted in 23 fatalities and more than 130 people were injured. Extensive damage to the plant facilities occurred (Figure 9 and Figure 10).

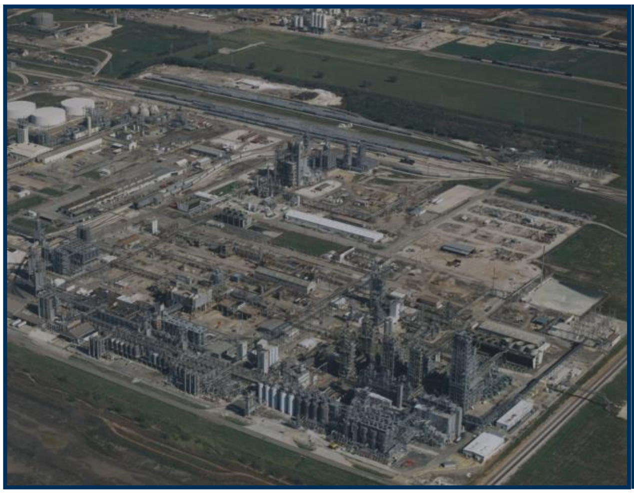


Figure 9. Philips complex before the accident

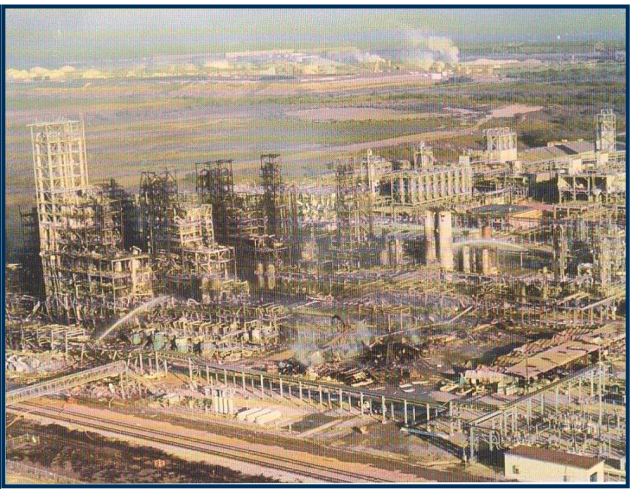


Figure 10. Philips complex after the accident

Since no one in direct control of the equipment/procedure involved in the release survived the explosion and because of the extensive damage caused, the exact sequence of the events was not determined. However, there were a few indications that the DEMCO valve opened (either by a human or a low-low-pressure trip signal in the reactor that caused the valve to open) while perhaps a shorter procedure was being used (settling pipe was disconnected, DEMCO valve was found open, air hoses were connected "in reverse", valve did not have the lock pin). Note that clearing a settling leg takes a minimum of 2 pipefitters (maintenance specialists) and one operator. The task involves completing steps very similar to "Lock-Out / Tag Out" (LOTO); double-blocking is not possible due to the nature of the polyethylene pluggage that must be cleared, so there is one 8-inch ball valve (DEMCO valve) between each setting leg and the reactor.

Scenario likelihood estimations

In this section we are going to ignore the information/details known from the investigation (as if we were in 1988, before the accident happened), and show different alternatives for the estimation of the accident frequency estimation. The scenario we are going to evaluate is **"DEMCO valve opens when the settling leg is disconnected during online maintenance"**.

The results are shown in Table 5 further below. Each case (method of calculation) is described on the two pages before Table 5.

Multiplying error per steps without any other HRA consideration (Incorrect)

Phillips did an initial estimation of the likelihood of the scenario in 1988 based on the "official" procedure (Table 4) and a basic human error probability for skipping a step of 1E-2, without considering potential dependence between the people involved in the online maintenance task. Philips obtained a likelihood/risk unrealistically low (less than 1 chance in a trillion years), whereas the accident occurred in 1989 just 15 years after commissioning.

A PHA Team with little/no knowledge on Human Reliability and Human Factors would probably come to a similar conclusion and therefore judged the risk to be tolerable.

LOPA: Using IEF lower limit from LOPA handbooks

Given that the unplugging procedure was performed more than a thousand times per year (per reactor), it can be considered that the lowest initiating event frequency (IEF) for the Human Error for single group of people is 1 per year (see *Guidelines for Initiating Events and IPLs*, 2015, CCPS/AIChE). This estimate gives an accident rate of about 1 per year to 1 in 10 years, which about right.

LOPA: Using LOTO lower limit

Like in the previous approach, for this simplified estimation the whole "unplugging procedure (operations + maintenance)" is considered a single "task". However, in this estimation a failure in the LOTO procedure is considered the Initiating Event (or because any equipment-based IPL would be considered in High Demand mode). For this estimation we have multiplied the LOTO PFD (1E-3) by the number of times that the procedure is used (8640 settling leg clearings per year), resulting in a likelihood of 8.6 accidents per year. This assumes that some failure occurs during the LOTO procedure for the settling leg resulting in the 8-inch ball valve coming open. 8.6 per year is much higher than that shown by the history of the plant, so likely one other failure is needed (such as random failure causing the 8-inch ball valve to open).

HRA: Simplified analysis of the Procedure

For this estimation, we have used the "Time at risk" concept and calculated the fraction of time in which the settling leg is disconnected. The IE considered was the valve opening, either mistakenly open by a human, valve failure, or a plant trip commanding the valve to open. As in the previous estimation, a PFD of 1E-3 was given to the LOTO procedure failure (grouping all the "safeguard" steps described in Table 4 and treating the group of 3-4 staff that clear a setting leg the same as one human

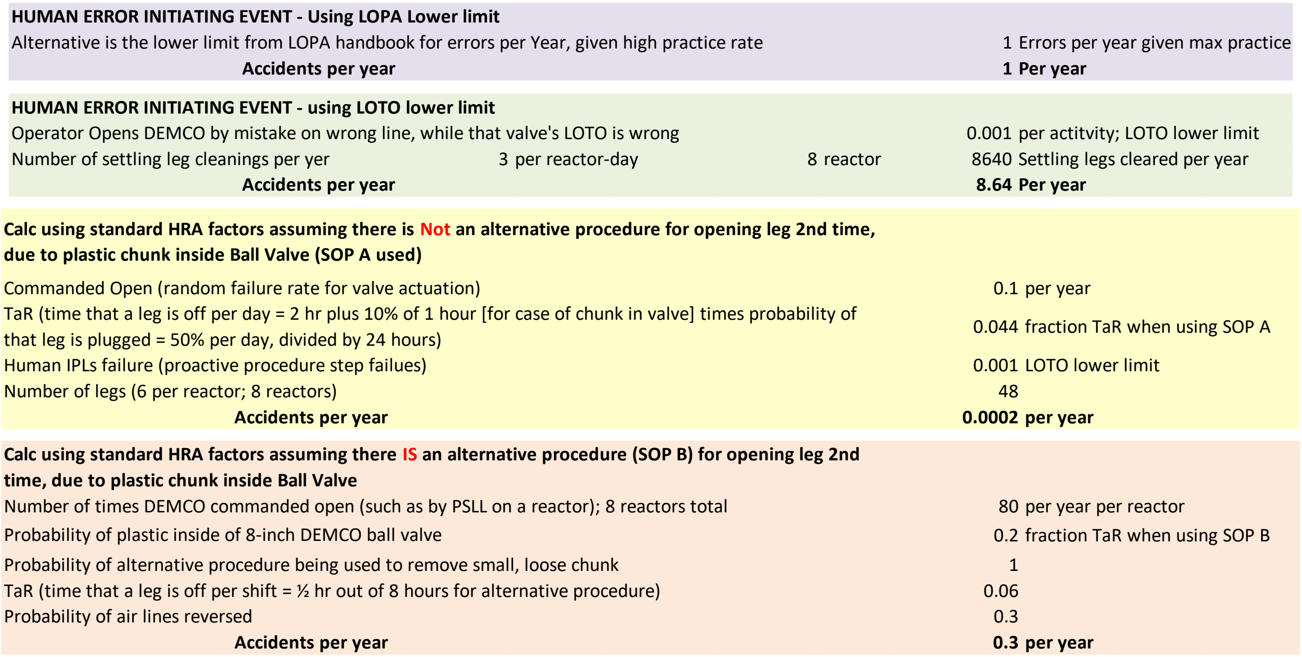
/squad). As can be seen in Table 5, the overall estimate by this method is 2 accidents per 10,000 years which is unrealistically low and does not match the accident history.

HRA: Simplified analysis of the "shortcut" procedure

This estimation is like the previous one, but with a lower amount of time of the settling leg disconnected. But this case also assumes that a chunk of plastic is cut off and retained inside the ball valve when it is closed, and when the valve is later opened after clearing the settling leg, the chunk of plastic shoots down the leg to the transition piece in the bottom of the settling leg. Further, if a PHA of procedures was properly conducted, the team likely would have discussed this possibility (which turns out that it occurs with 10% of the clearings) and would have likely discussed that there is an unwritten procedure to allow quicker removal of this chunk without having to fully disassemble the settling leg. We assumed (without proof) for this example that the only safeguard left in place to keep the 8-inch valve closed is the closure of the local manual switch at the valve station. Further, we assumed that wiring errors were made that would allow a PSLL in the reactor to override the local switch and open the 8-inch ball valve (assuming the airlines are also reversed for opening and closing). Both of these assumptions were discussed in the PHA of the rebuild the plant (for new Plant 6) and deemed more likely than other possibilities. The accident frequency for this case was 3 releases in 10 years, which very closely matches 1 accident in 15 years.

Results comparison/summary

Table 5. Likelihood estimations summary for Phillips Disaster



HUMAN ERROR INITIATING EVENT - Using LOPA Lower limit						
Alternative is the lower limit from LOPA handbook for errors per Year, given high practice rate					1	Errors per year given max practice
Accidents per year					**1**	**Per year**
HUMAN ERROR INITIATING EVENT - using LOTO lower limit						
Operator Opens DEMCO by mistake on wrong line, while that valve's LOTO is wrong					0.001	per actitvity; LOTO lower limit
Number of settling leg cleanings per yer	3	per reactor-day	8	reactor	8640	Settling legs cleared per year
Accidents per year					**8.64**	**Per year**
Calc using standard HRA factors assuming there is Not an alternative procedure for opening leg 2nd time, due to plastic chunk inside Ball Valve (SOP A used)						
Commanded Open (random failure rate for valve actuation)					0.1	per year
TaR (time that a leg is off per day = 2 hr plus 10% of 1 hour [for case of chunk in valve] times probability of that leg is plugged = 50% per day, divided by 24 hours)					0.044	fraction TaR when using SOP A
Human IPLs failure (proactive procedure step failues)					0.001	LOTO lower limit
Number of legs (6 per reactor; 8 reactors)					48	
Accidents per year					**0.0002**	**per year**
Calc using standard HRA factors assuming there IS an alternative procedure (SOP B) for opening leg 2nd time, due to plastic chunk inside Ball Valve						
Number of times DEMCO commanded open (such as by PSLL on a reactor); 8 reactors total					80	per year per reactor
Probability of plastic inside of 8-inch DEMCO ball valve					0.2	fraction TaR when using SOP B
Probability of alternative procedure being used to remove small, loose chunk					1	
TaR (time that a leg is off per shift = ½ hr out of 8 hours for alternative procedure)					0.06	
Probability of air lines reversed					0.3	
Accidents per year					**0.3**	**per year**

For this Phillips it turns out that using the standard LOPA factor of 1 human error per year, assuming high practice rate per group of persons (3 to 4 staff) per year (more than 2000 practices per year per shift) gives approximately the same answer as a simplified HRA. Further, assuming there is no alternative procedure for removing a chunk of plastic from the bottom of the settling leg (after opening the 8-inch ball valve) is not a practical assumption as it does not match the actual accident rate of 1 per 15 years. Finally, the PHA of the procedures for startup, shutdown, and online maintenance was crucial for uncovering the most likely scenarios for the errors that occurred on the day of the accident.

NOTE: A detailed HRET was completed to comply with the settlement agreement, but it gave essentially the same results as using the lower limits allowed in LOPA for human error probability for LOPA.

Case study 02: Copper smelter

In the copper smelting process shown in Figure 11, the equipment is run at a few inches of vacuum. SO_2 gas (up to 40% by wt.) is generated from the copper sulfate ore; SO_2 is strongly corrosive to lungs, eyes, and throat tissue. There are many locations in the process that commonly plug with ore or dust. When this occurs, the performance of the smelter drops noticeably. To remedy the situation, operators open a door, hatch, or port on the smelter equipment and manually clear the buildup using long rods. While the equipment is open, the control room adjusts the draft to prevent positive pressure which would release hot, SO_2 rich gas out the doorway, hatch, or port.

Table 6 shows typical steps for clearing pluggages within the smelter process. There are No IPLs to protect the workers; only multiple human actions and precautions (non-IPLs) are typically in place. Table 7 shows the HRA summary from a HAZOP / LOPA that was incompetently performed one year before a fatality occurred. Also, in Table 7, is a summary of an HRA performed by a competent HAZOP / LOPA team with a PHA/LOPA facilitator that is expert in human factors and human reliability.

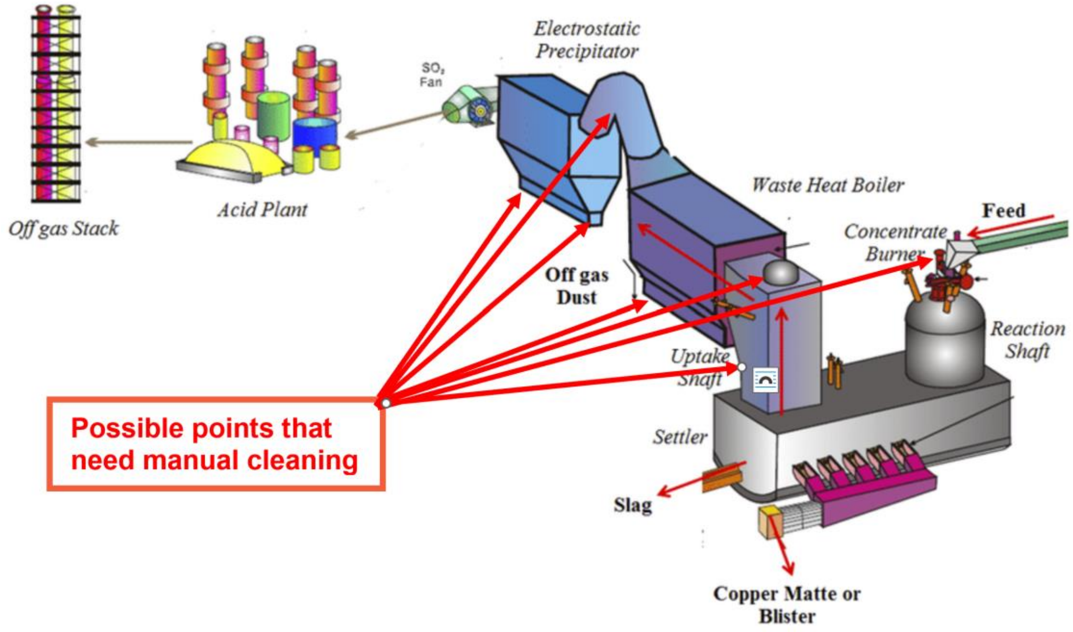


Figure 11. Copper smelter scheme

Table 6. Online Maintenance SOP – Opening Access ports / doors and remove ore or dust pluggage.

#	Task
1	Collect necessary tools, wrenches, hammers, rods, pry bars, chisels
2	Check in with control room so they know when to increase suction compressor / fan or adjust dampers to maintain draft
3	Equipment Operator start breathing air supply to hood and put on hood
4	Second Operator (watch) start breathing air supply to hood and put on hood
5	Enter the room of the building where the work will occur
6	Unlatch the door or port and open fully nearest the suspected pluggage
7	Visually confirm the draft is sufficient to prevent SO2 gas from escaping
8	Do work to clear plug
9	Close door / port
10	Tell Control Room the work is complete
WARNING: If during any part of the work you see / sense loss of draft, or smell strong SO2 odor, then stop work immediately and exit that part of the building and call control room to report the situation.	

Table 7. Likelihood estimations summary for Copper Smelter

	PHA by Poor leader/team	PII: PHA + LOPA + HRA	After PII Recs to date	After PII Recs by 12/23
Chute plugged with ore; 1/day	365	365	365	365
Operator fails to don hood with supplied breathing air	0.01	0.1	0.1	0.1
Probability of Second Operator failing to don breathing air	0.01	0.95	0.95	0.95
Operator opens door to clean chute	1	1	1	1
Combined HE Probability	0.0001	0.0950	0.0950	0.0950
Time at risk for compressor failure 1 hr per day	0.0417	0.0417	0.0417	0.0417
Initiating Event - suction compressor fails/ per year	30	30	3	0.1
Failure of Operator to smell SO2 and quickly exist	0.1	1	1	1
Interlock to not allow Large door to open unless Ore feeding is shut down 1 minute prior	NA	NA	0.1	0.1
Interlock to shut down feeding ore if doors open	NA	NA	1 (not IPL)	1 (not IPL)
Interlock to shut down feeding ore when compressor shuts down	NA	NA	0.1	0.1
Probability of Accident per Yr	**1.3E-05**	**0.12**	**1.2E-04**	**4.0E-06**
Current RRF	**80,000**	**8**	**8,421**	**252,632**
RRF needed (to reach RRF of 10,000 or to reach TMEL 10-4/yr)	**0**	**1200**	**1.2**	**0**
Years of Operation	40	40	40	40
Probability of Accident Once in Operating period to date	**5.E-04**	**4.75**	**5.E-03**	**2.E-04**

The incompetent PHA team leader resulted in the company judging the frequency of fatality to be 5 in 10,000 years, even though there were no IPLs. All of the human protections were counted as IPLs with a PFD of 0.01 chance of failure. If this PHA/LOPA had been performed competently, the risk would have been 10,000 times higher and likely the copper smelting company would have taken many steps to limit the risk near-term as true IPLs were developed and as the IEF was reduced.

The competent team / analysts that re-did the PHA/LOPA immediately after the accident judged the frequency of a fatality at about 5 per year, a difference of 4 orders of magnitude. Then, the site accepted the recommendation to reduce the risk by greatly improving the reliability of the draft control fan (compressor) thereby reducing the IEF and by adding IPLs to ensure the SO_2 generation is cut quickly if the draft is lost for any reason. The final risk control measure should reduce the risk to the acceptable range of 2 per 10,000 years (with proven independence of all IPLs).

The main lesson: Never hire a PHA/LOPA leader who is not competent in human reliability and also ensure the PHA covers all modes of operation as required by CCPS, US CSB, and US OSHA.

Case study 03: SIL Verification

Human error rates must also be accounted for in the estimation of the PFD for any IPL. The most difficult case is for a SIF of high SIL. The following examples build upon the paper titled *SIL 2, SIL 3, and Unicorns* that the authors presented at this conference in 2019. [8]

Example 01: Illustration of Estimate of PFD_{SIF}, for a SIL 1 SIF, with and without consideration of P_{HUM}

For the SIL 1 SIF in Figure 12, the component PFDs were estimated using standard, simplified equations for each, and using generic data available for the components. Based on this calculation, the PFD of the SIF without consideration of discrete systematic error yielded a $PFD_{COMP} = 0.039$.

For this example, the term $\sum P_{HUM}$ is next estimated by summing the:

- Probability of leaving the root valve for the level switch (sensor/transmitter) closed
- Probability of leaving the entire SIF in BYPASS after maintenance or after some other human intervention (such as an inadvertent error or as a necessity during startup)
- Probability of miscalibration of the level transmitter/switch.

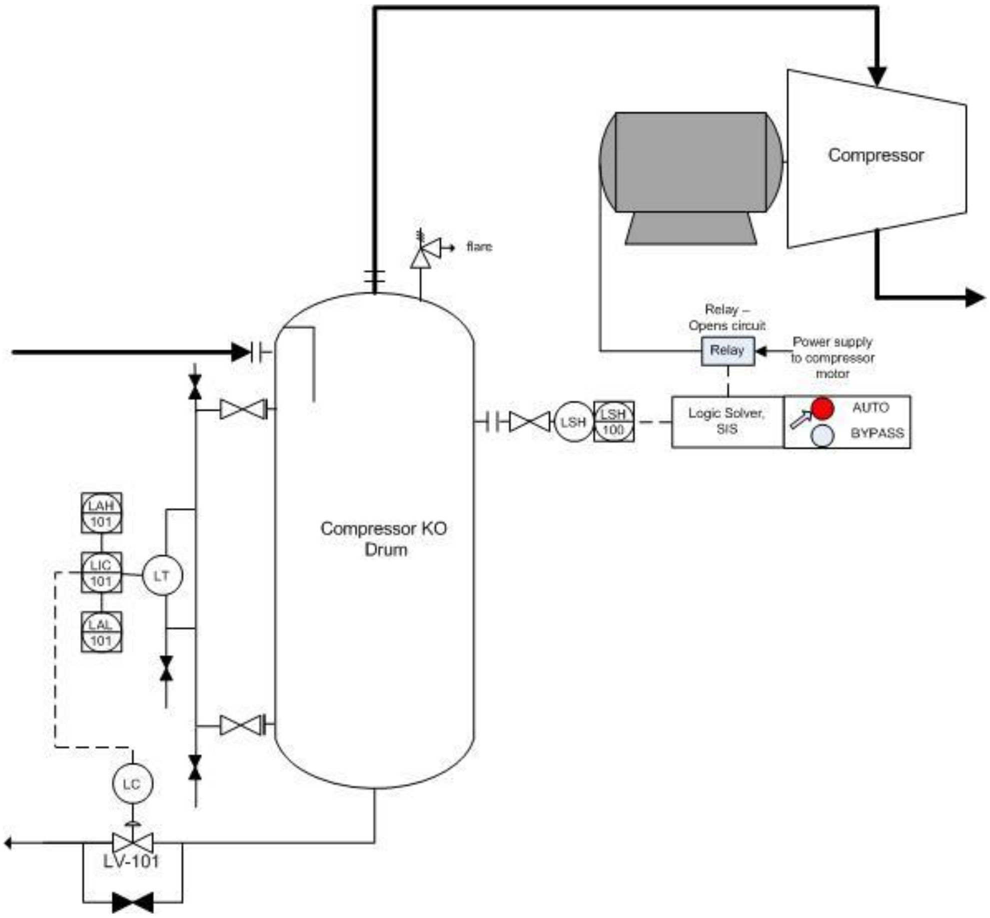


Figure 12. Example of SIL 1 SIF (high level trip of compressor motor)
Courtesy Process Improvement Institute, Inc., All Rights Reserved

Since these are all independent specific errors, the error rate will simply be 0.02 (the base error probability provided) for each mistake, or:

$$\sum P_{HUM} = P_{RV\ closed} + P_{SIF\ left\ bypassed} + P_{miscalibration} = 0.02 + \ 0.02 + 0.02 = 0.06 \qquad \text{[Eq. 6]}$$

This would then give an overall failure probability for the SIF of:

$$PFD_{SIF} = \ PFD_{COMP} + PFD_{HUM} = 0.039 + 0.06 = 0.099 \qquad \text{[Eq. 7]}$$

Since the PFD_{SIF} is less than 0.1, the instrumented system for high level protection still qualifies as a SIL 1 SIF. But suppose we wish to improve the reliability and independence of the instrumented system by using a smart sensor/transmitter for the high-level switch (LSH) which will detect null movement of the sensor reading (indicating the root valve is closed or the tap is plugged) or suppose we put a limit switch (or captive key system) on the root valve. There is a probability that these safeguards against human error will also fail or be bypassed by the staff, but assuming the probability of that failure is the same as other human errors for this example, 0.02, then the overall system human error is reduced, because the probability of leaving the root valve closed is now ANDed with the probability of smart sensor/transmitter or limit switch failing:

$$\sum P_{HUM} = (0.02 \times 0.02) + 0.02 + 0.02 = 0.04 \quad \text{[Eq. 8]}$$

Therefore, the revised PFD of the instrumented system becomes:

$$PFD_{SIF} = PFD_{COMP} + PFD_{HUM} = 0.039 + 0.04 = 0.079 \quad \text{[Eq. 9]}$$

Sensitivity to Baseline Human Error Rate: If the baseline human error probability increases to 0.04 due to fatigue or extra stress due to schedule constraints, then even with the extra instrumentation to detect valve closure, the PFD of the systematic human error will increase substantially:

$$\sum P_{HUM} = (0.04 \times 0.04)\ +\ 0.04\ +\ 0.04\ =\ 0.082 \quad \text{[Eq. 10]}$$

The revised PFD of the instrument system becomes:

$$PFD_{SIF}\ =\ PFD_{COMP} + PFD_{HUM} = 0.039\ +\ 0.082\ =\ 0.121 \quad \text{[Eq. 11]}$$

In this modified case, which is applicable to about a third of the facilities PII has visited in the past 10 years (due primarily to fatigue), the instrumented system no longer qualifies as a SIL 1.

NOTE: IEC 61511 does NOT require consideration of specific human errors in SIL Verification, opting instead to state "the end users must eliminate human error of interventions with the SIF". The authors note that if the industry could eliminate human error, then SIFs would be unnecessary.

The human error for miscalibration is challenging to reduce, unless there are redundancy and voting of the level sensor/transmitters; then miscalibration errors can be essentially eliminated as an important contribution to human error. This case will be explored as part of Example 02. However, the redundancy and voting of transmitters cannot detect an error introduced by using the same calibrator (hardware) that has some error (drift).

The composite error of leaving the entire system in bypass is usually made up of:

1. The inadvertent error to return the system to AUTO after maintenance (a good design would generate a recurring alarm for an SIF in bypass, and a good management system would track and correct such alarms), and
2. The probability that the staff will make the intentional decision to leave the SIF in bypass, for perhaps a reason not anticipated by the designers. Management of change (MOC) should address the latter case; a strong MOC system should have multiple personnel who would cross-check each other. A bigger issue is failing to recognize that an MOC is needed. Other issues could be the company does not require a mini-PHA to be performed for changes to steps in a procedure.

Therefore, this error rate potentially can be reduced by adding repeating alarms to alert the staff that the SIF is still bypassed. A strong management system is essential, else the staff may hear and acknowledge the alarms, but will leave the system in bypass intentionally. Thus, it is critical that the designers anticipate the need for a bypass (such as during startup) and that they provide an appropriate startup bypass that resets the SIF automatically after (for instance) 60 minutes.

Example 02: Illustration of Estimate of PFD_{SIF}, for a SIL 2 SIF, with and without consideration of P_{HUM}

For the SIL 2 SIF described in Figure 13, the component PFDs were estimated using standard, simplified equations for each, and using available industry data for the components. For the case where the sensors are voted 2oo3, the PFD of the SIF without consideration of specific human error yielded PFD_{COMP} = 0.008.

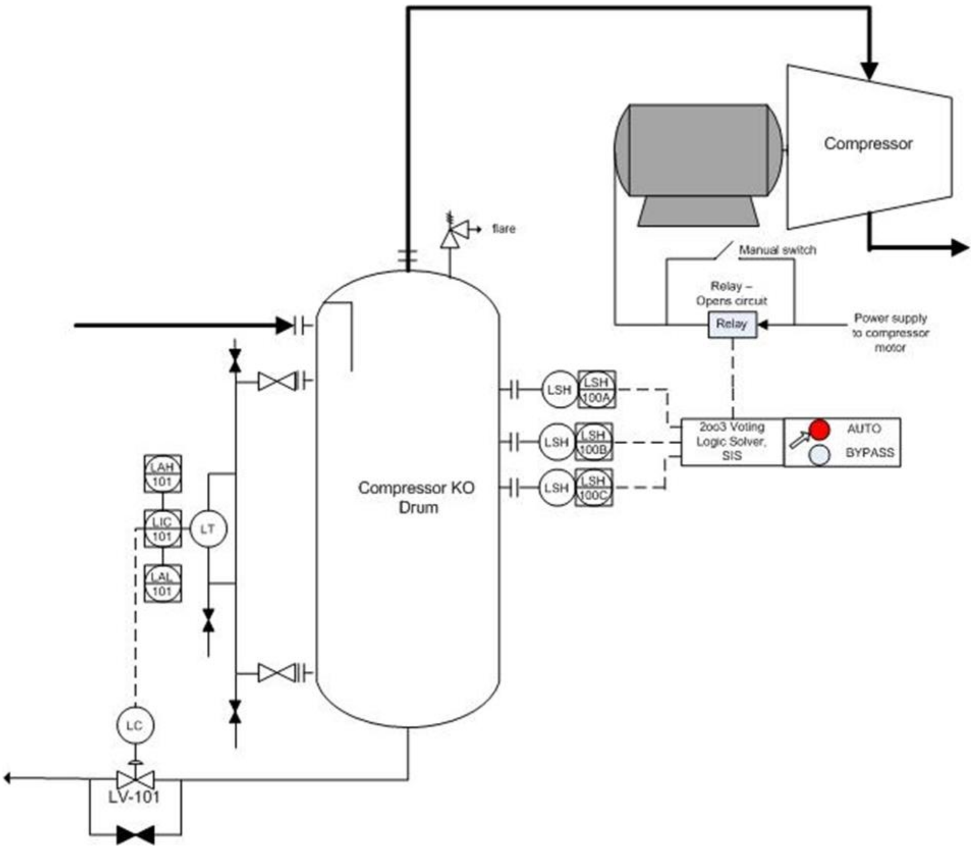


Figure 13. Example of SIL 2 SIF (high level trip of compressor motor)
Courtesy Process Improvement Institute, Inc., All Rights Reserved

For this example, the term $\sum P_{HUM}$ is next estimated by summing the:

- Probability of leaving the level sensor/transmitters 2oo3 root valves closed, causing an unsafe failure. (This calculation is shown later.)
- Probability of miscalibration of the level transmitter/switch. This calculation is shown later, but for this issue to be a significant probability, two of the three or else all three of the sensors/transmitters

must be mis-calibrated, unless there is comparison checking, then it would require miscalibration of all three transmitters.

- Probability of leaving the entire SIF in BYPASS after maintenance or after some other human intervention such as an error or a necessity during startup; as before, we will use the base error probability of 0.02 as a starting point.
- Probability of leaving the relay bypass closed. As before, we will use the base error probability of 0.02 as a starting point.

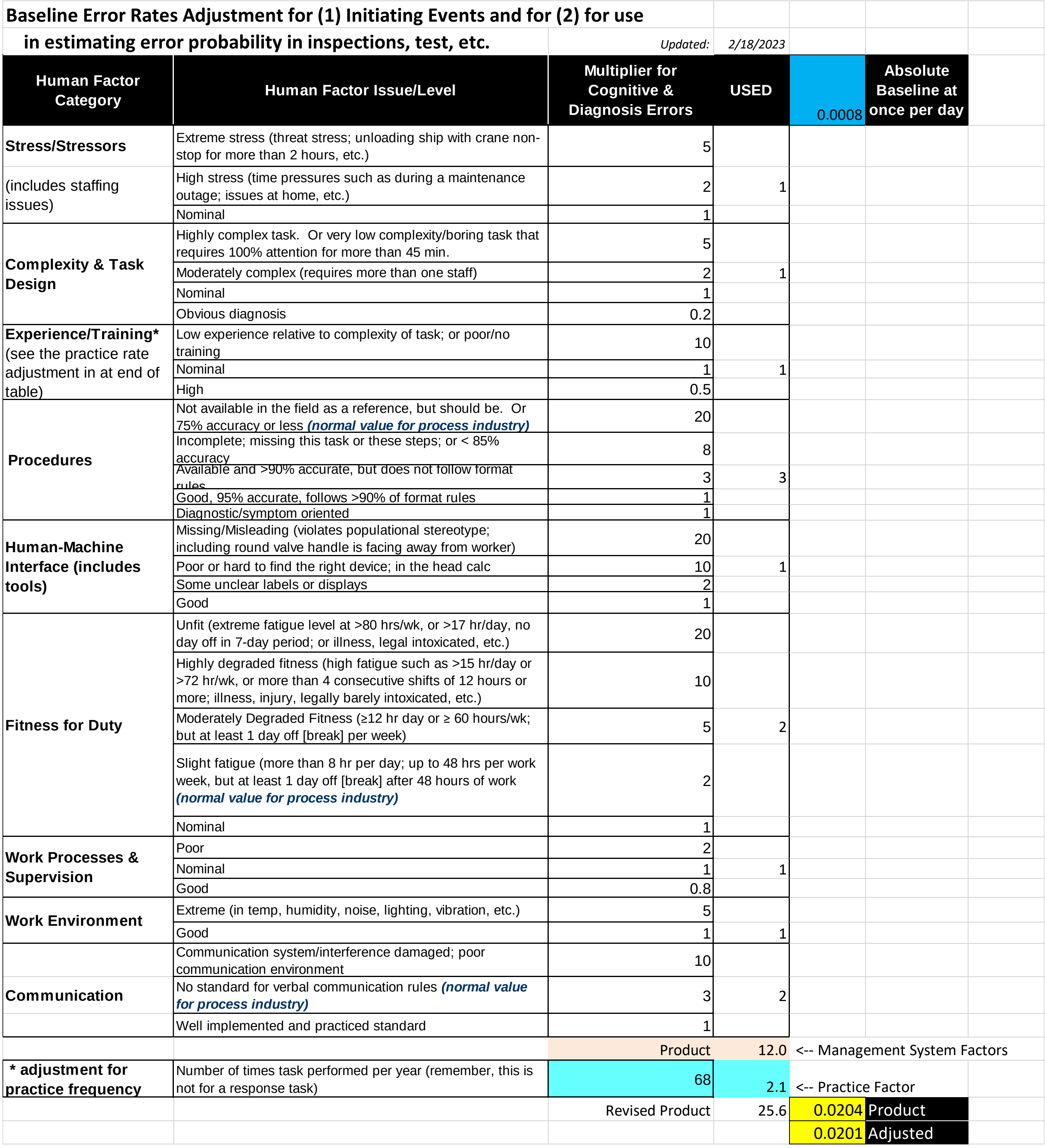
$$\sum P_{HUM} = P_{root\ valve} + P_{miscal} + P_{SIF\ bypass} + P_{relay\ bypass} \qquad \text{[Eq. 12]}$$

Baseline error calculation.

02

Table 8 shows the calculation of the Baseline Human Error using the Human Factors table (Table 1) and adjusting the value based on the practice rate of 68 activities per year per operator and per instrument technician.   The calculated Baseline Human Error Rate is 0.02

Table 8. Baseline error rate calculation. Practice rate: 68 activities per year.
Courtesy Process Improvement Institute, Inc., All Rights Reserved



Baseline Error Rates Adjustment for (1) Initiating Events and for (2) for use					
in estimating error probability in inspections, test, etc.		Updated:	2/18/2023		
Human Factor Category	Human Factor Issue/Level	Multiplier for Cognitive & Diagnosis Errors	USED	0.0008	Absolute Baseline at once per day
Stress/Stressors	Extreme stress (threat stress; unloading ship with crane non-stop for more than 2 hours, etc.)	5			
(includes staffing issues)	High stress (time pressures such as during a maintenance outage; issues at home, etc.)	2	1		
	Nominal	1			
Complexity & Task Design	Highly complex task. Or very low complexity/boring task that requires 100% attention for more than 45 min.	5			
	Moderately complex (requires more than one staff)	2	1		
	Nominal	1			
	Obvious diagnosis	0.2			
Experience/Training* (see the practice rate adjustment in at end of table)	Low experience relative to complexity of task; or poor/no training	10			
	Nominal	1	1		
	High	0.5			
Procedures	Not available in the field as a reference, but should be. Or 75% accuracy or less ***(normal value for process industry)***	20			
	Incomplete; missing this task or these steps; or < 85% accuracy	8			
	Available and >90% accurate, but does not follow format rules	3	3		
	Good, 95% accurate, follows >90% of format rules	1			
	Diagnostic/symptom oriented	1			
Human-Machine Interface (includes tools)	Missing/Misleading (violates populational stereotype; including round valve handle is facing away from worker)	20			
	Poor or hard to find the right device; in the head calc	10	1		
	Some unclear labels or displays	2			
	Good	1			
Fitness for Duty	Unfit (extreme fatigue level at >80 hrs/wk, or >17 hr/day, no day off in 7-day period; or illness, legal intoxicated, etc.)	20			
	Highly degraded fitness (high fatigue such as >15 hr/day or >72 hr/wk, or more than 4 consecutive shifts of 12 hours or more; illness, injury, legally barely intoxicated, etc.)	10			
	Moderately Degraded Fitness (≥12 hr day or ≥ 60 hours/wk; but at least 1 day off [break] per week)	5	2		
	Slight fatigue (more than 8 hr per day; up to 48 hrs per work week, but at least 1 day off [break] after 48 hours of work ***(normal value for process industry)***	2			
	Nominal	1			
Work Processes & Supervision	Poor	2			
	Nominal	1	1		
	Good	0.8			
Work Environment	Extreme (in temp, humidity, noise, lighting, vibration, etc.)	5			
	Good	1	1		
Communication	Communication system/interference damaged; poor communication environment	10			
	No standard for verbal communication rules ***(normal value for process industry)***	3	2		
	Well implemented and practiced standard	1			
		Product	12.0	<-- Management System Factors	
* adjustment for practice frequency	Number of times task performed per year (remember, this is not for a response task)	68	2.1	<-- Practice Factor	
		Revised Product	25.6	0.0204	Product
				0.0201	Adjusted

Root valves closed.

To aid in the calculation of the probability of leaving 2oo3 root valves closed, we use an event tree to show the conditional probabilities for leaving Valve B closed, given Valve A is open or closed, and similarly, the conditional probability of leaving Valve C closed, given Valve A or B are closed or both Valve A and B are closed. Figure 14 shows the HRET for this case and the results of this calculation. For the branch probabilities, the equations for high dependency (HD) of the human actions were used (see Table 3); this tree reflects the more prevalent case of redundant channels being maintained on the same day, by the same person, and that level valves are within the visual field of the worker. From Figure 14 the result for the probability of human error of leaving 2oo3 or 3oo3 of the root valves closed can be calculated, and a theoretically dangerous outcome. But the comparison checking between sensors/transmitters will alert the workers that a root valve is closed (assuming 100% detection and correction), so the only valid path is the 3oo3 path; the 3oo3 error case is the bottom row of the event tree in Figure 14. The probability of leaving all three root valves closed is 0.0052.

Figure 15 shows the effect of staggering maintenance by using the Low Dependency equations (from Table 3) on the event tree. For the Low Dependency case, the probability of leaving all three root valves closed is 9.6E-5.

Sensors Mis-calibrated.

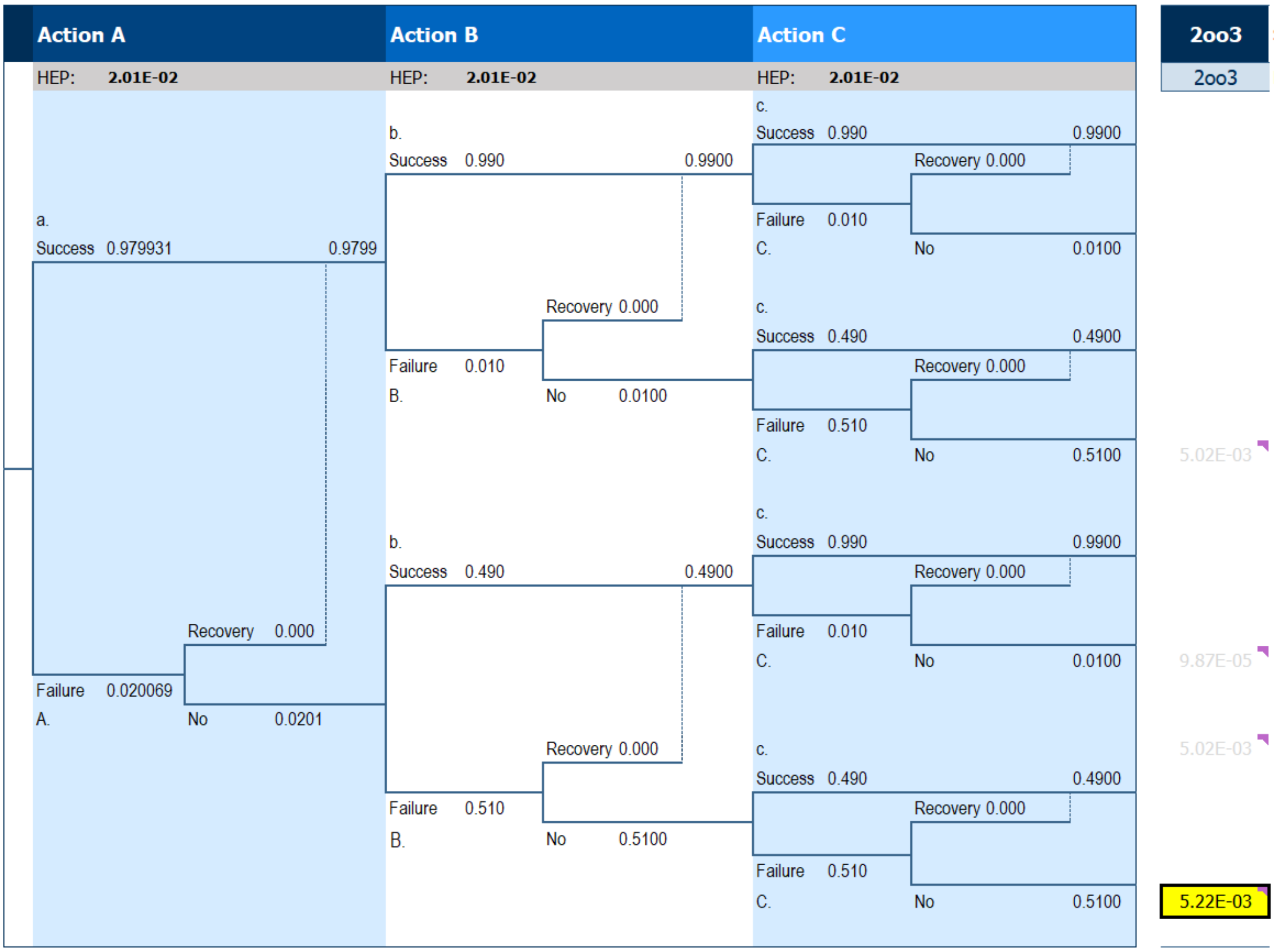
From the same figure (Figure 14), we can also extract the conditional probability of leaving 3oo3 sensors/transmitters bypassed; assuming comparison checking is in place to note deviations and correct the problem, only the case of 3oo3 errors is applicable. This represents a strong recovery path for the previous errors (95% detection and correction). The 3oo3 error case is the bottom row of the event tree in Figure 14. The probability of miscalibrating all three sensors/transmitters is 0.0052.

$$\sum P_{HUM} = 0.0052 + 0.0052 + 0.02 + 0.02 = 0.0504 \qquad \text{[Eq. 13]}$$

This contribution would then give an overall failure probability for the SIF of:

$$PFD_{SIF} = PFD_{COMP} + PFD_{HUM} = 0.008 + 0.0504 = 0.058 \qquad \text{[Eq. 14]}$$

Since the PFD_{SIF} is greater than 0.01, the instrumented system for high level protection in this example does not qualify as a SIL 2 SIF when accounting for human error probabilities related to interventions with the SIF.



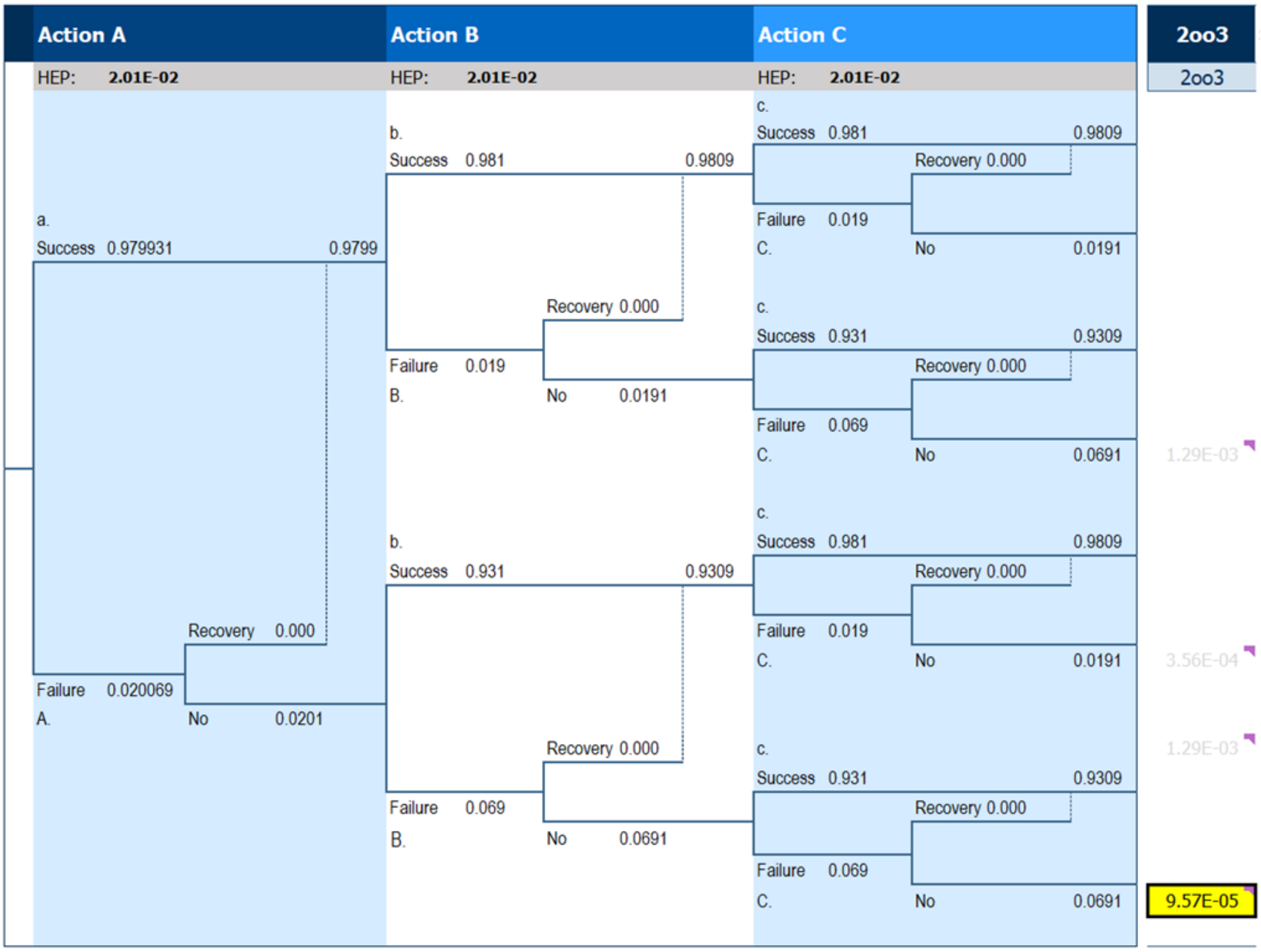
Event tree applies to Actions:
- Opening Sensor A/B/C root valve after maintenance
- Calibrating Sensor A/B/C
- Removing bypass from device A/B/C

Figure 14. Calculation of Conditional Probability of Failure in 2oo3 Actions
BHEP: 0.02 – High Dependency
Courtesy Process Improvement Institute, Inc., All Rights Reserved

Detection and Correction of Sensor Errors

One means to improve the reliability and independence of the instrumented system is to use a smart sensor/transmitter for the LSH which will detect null movement of the sensor reading, indicating the valve is closed or the tap is plugged. Another possibility is to implement a limit switch (or captive key system) on the root valve. There is a probability that these safeguards against human error will also fail or be bypassed by the staff, but assuming the probability of that failure is the same as other human errors for this example, 0.02, then the systemic human error drops to about zero as the probability of leaving the root valve closed is now ANDed with the probability of smart sensor/transmitter or limit switch failing, as shown in Table 10.

$$\sum P_{HUM} = P_{root\ valve} + P_{miscal} + P_{SIF\ bypass} + P_{relay\ bypass}$$
$$= 0.0001 + 0.0001 + 0.02 + 0.02 = 0.0402$$
[Eq. 15]



Event tree applies to Actions:
- Opening Sensor A/B/C root valve after maintenance
- Calibrating Sensor A/B/C
- Removing bypass from device A/B/C

Figure 15. Calculation of Conditional Probability of Failure in 2oo3 Actions
BHEP: 0.02 – Low Dependency
Courtesy Process Improvement Institute, Inc., All Rights Reserved

Since the PFD_{SIF} is greater than 0.01, the instrumented system for high level protection still does not qualify as a SIL 2 SIF when accounting for human error probabilities related to interventions with the SIF. The weak link in this design is again the human error probability of leaving either the relay bypass closed or the probability of leaving the entire SIF bypassed. This is a common concern on all SIFs that have system bypasses. The most effective way to drop these error rates is to eliminate the capability for bypassing the relay and to eliminate the capability for bypassing the entire SIF. Or we can install a parallel relay with a selector switch so that one relay (and only one) is aligned in the circuit to the motor of the compressor. This will likely drop the relay systemic human error probability from 0.02 down to 0.0004 or lower. The toughest bypass to eliminate is the one for the entire SIF which is only feasible on batch systems or on continuous operations that can be shut down completely for each test interval. However, again, a design with a recurring alarm on bypass and a strong management system to correct the alarm could reduce the bypassed SIF probability to 0.0004 or lower. This change could achieve SIL 2 PFD.

$$\sum P_{HUM} = P_{root\ valve} + P_{miscal} + P_{SIF\ bypass} + P_{relay\ bypass} \\ = 0.00016 + 0.00016 + 0.0004 + 0.0004 = 0.001 \qquad \text{[Eq. 16]}$$

This would then give an overall failure probability for the SIF of

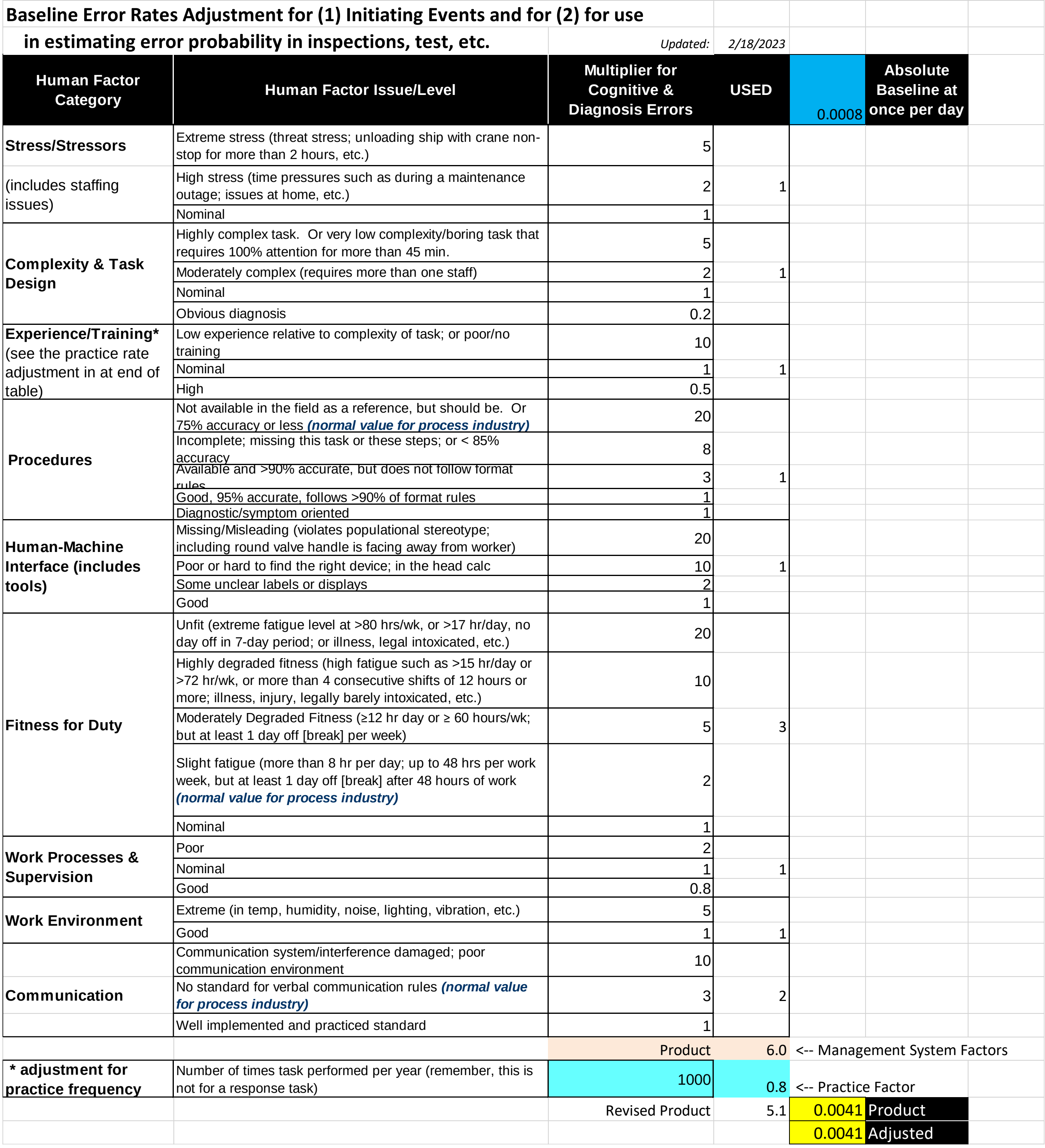
$$PFD_{SIF} = PFD_{COMP} + PFD_{HUM} = 0.008 + 0.001 = 0.009 \qquad \text{[Eq. 17]}$$

Sensitivity to baseline human error rate.

Obviously, if the baseline human error probability increases to 0.04 due to extra fatigue or extra stress due to schedule constraints, the PFD of the systematic human error will increase substantially and the SIL 2 target becomes even less attainable.

On the other hand, the error rate could be lowered if the practice rate was higher. PII collected data from 5 large petrochemical sites that indicated that on average, an instrument technician performs about 1000 test, checks, and/or calibrations per year. (Note that each plant is older than 15 years.) Table 9 shows the calculation of the Baseline Human Error using the Human Factors table (Table 1) and adjusting the value based on an increased practice rate of 1000 activities per year. The calculated Baseline Human Error Rate is 0.0041 (1/20th of the previous example).

Table 9. Baseline error rate calculation. Practice rate: 1000 activities per year
Courtesy Process Improvement Institute, Inc., All Rights Reserved

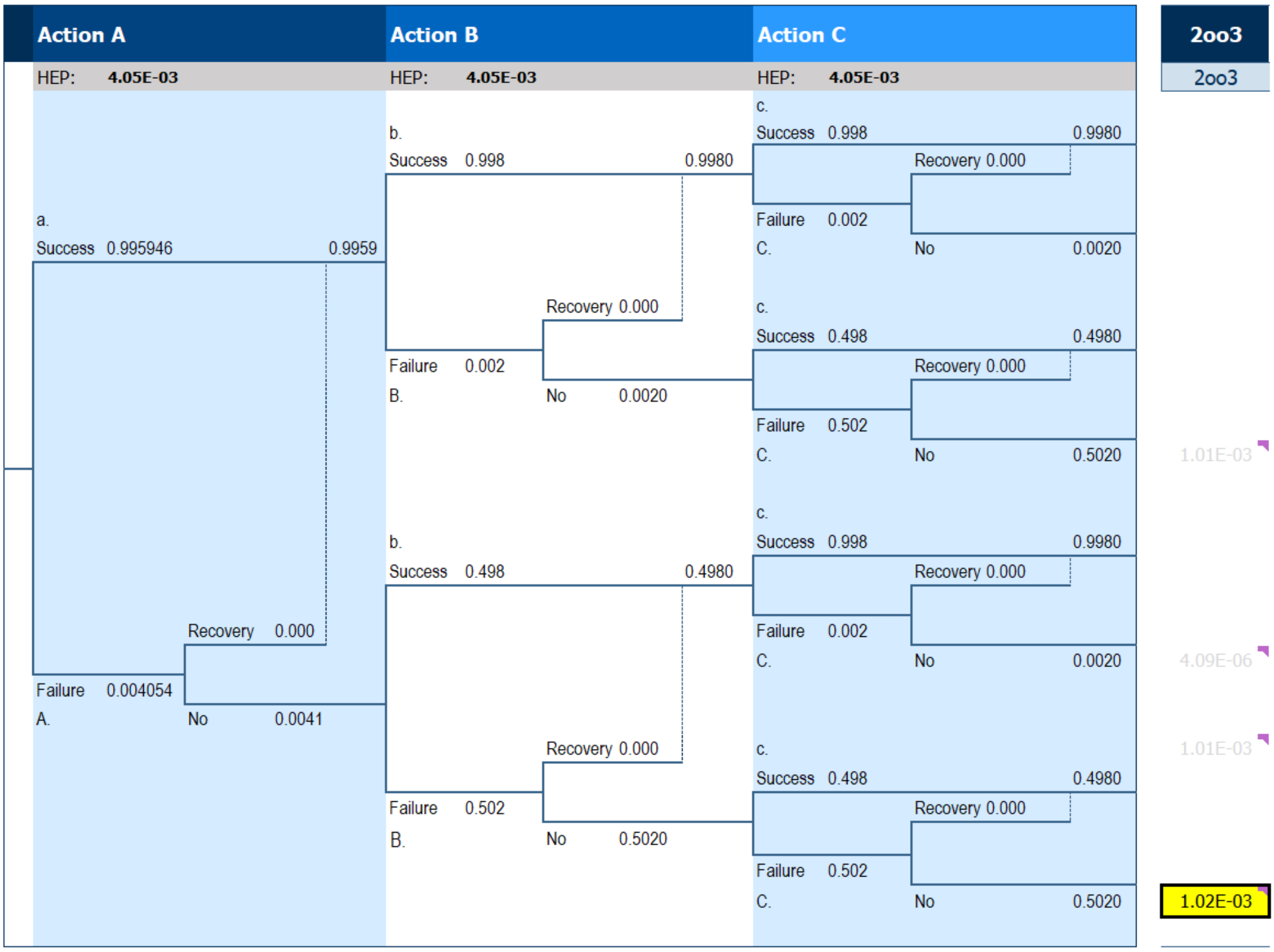


Baseline Error Rates Adjustment for (1) Initiating Events and for (2) for use
in estimating error probability in inspections, test, etc.

Updated: *2/18/2023*

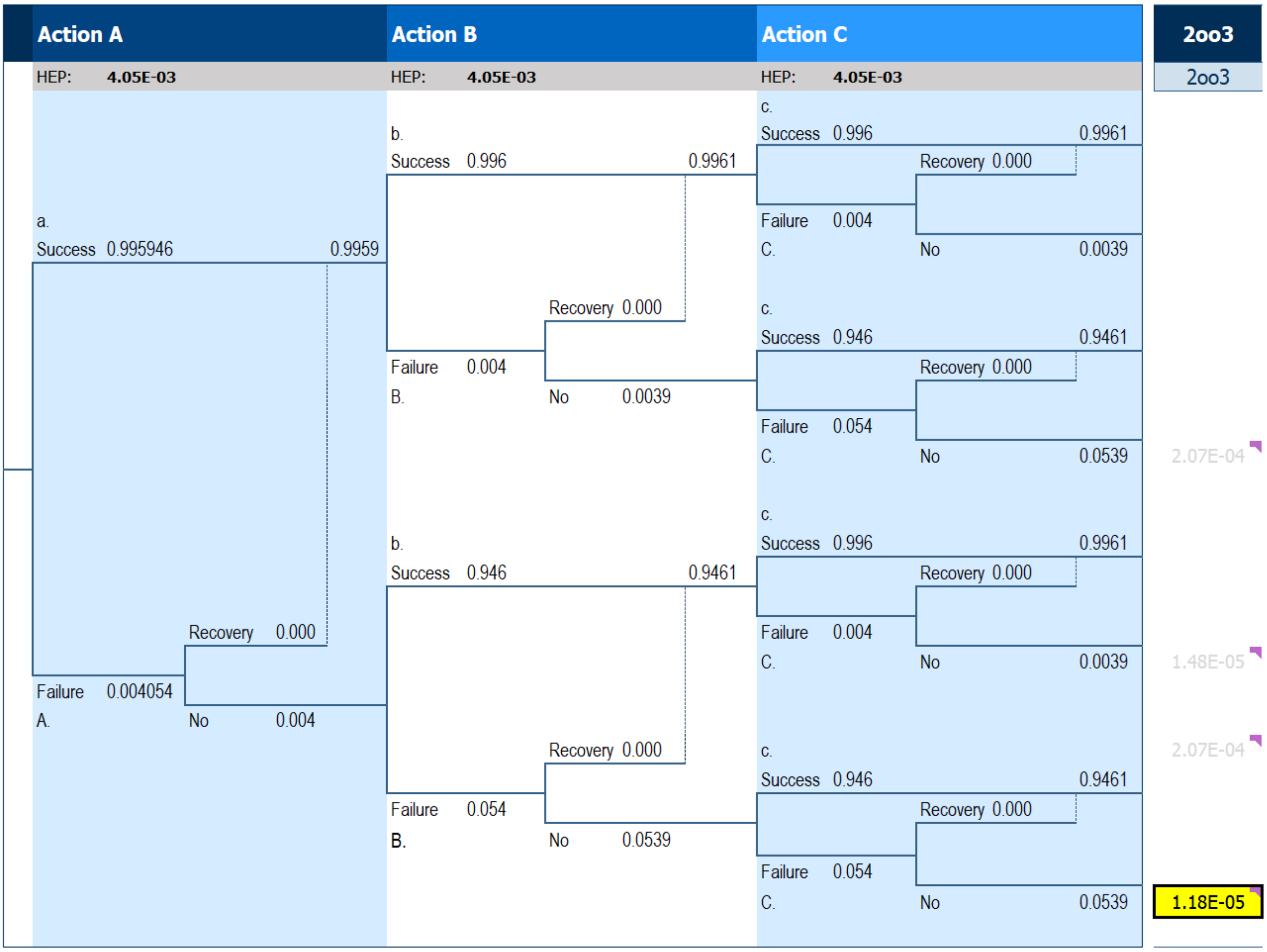
Human Factor Category	Human Factor Issue/Level	Multiplier for Cognitive & Diagnosis Errors	USED	0.0008	Absolute Baseline at once per day
Stress/Stressors	Extreme stress (threat stress; unloading ship with crane non-stop for more than 2 hours, etc.)	5			
(includes staffing issues)	High stress (time pressures such as during a maintenance outage; issues at home, etc.)	2	1		
	Nominal	1			
Complexity & Task Design	Highly complex task. Or very low complexity/boring task that requires 100% attention for more than 45 min.	5			
	Moderately complex (requires more than one staff)	2	1		
	Nominal	1			
	Obvious diagnosis	0.2			
Experience/Training* (see the practice rate adjustment in at end of table)	Low experience relative to complexity of task; or poor/no training	10			
	Nominal	1	1		
	High	0.5			
Procedures	Not available in the field as a reference, but should be. Or 75% accuracy or less ***(normal value for process industry)***	20			
	Incomplete; missing this task or these steps; or < 85% accuracy	8			
	Available and >90% accurate, but does not follow format rules	3	1		
	Good, 95% accurate, follows >90% of format rules	1			
	Diagnostic/symptom oriented	1			
Human-Machine Interface (includes tools)	Missing/Misleading (violates populational stereotype; including round valve handle is facing away from worker)	20			
	Poor or hard to find the right device; in the head calc	10	1		
	Some unclear labels or displays	2			
	Good	1			
Fitness for Duty	Unfit (extreme fatigue level at >80 hrs/wk, or >17 hr/day, no day off in 7-day period; or illness, legal intoxicated, etc.)	20			
	Highly degraded fitness (high fatigue such as >15 hr/day or >72 hr/wk, or more than 4 consecutive shifts of 12 hours or more; illness, injury, legally barely intoxicated, etc.)	10			
	Moderately Degraded Fitness (≥12 hr day or ≥ 60 hours/wk; but at least 1 day off [break] per week)	5	3		
	Slight fatigue (more than 8 hr per day; up to 48 hrs per work week, but at least 1 day off [break] after 48 hours of work ***(normal value for process industry)***	2			
	Nominal	1			
Work Processes & Supervision	Poor	2			
	Nominal	1	1		
	Good	0.8			
Work Environment	Extreme (in temp, humidity, noise, lighting, vibration, etc.)	5			
	Good	1	1		
Communication	Communication system/interference damaged; poor communication environment	10			
	No standard for verbal communication rules ***(normal value for process industry)***	3	2		
	Well implemented and practiced standard	1			
		Product	6.0	<-- Management System Factors	
* adjustment for practice frequency	Number of times task performed per year (remember, this is not for a response task)	1000	0.8	<-- Practice Factor	
		Revised Product	5.1	0.0041	Product
				0.0041	Adjusted

Figure 16 (High dependency) and Figure 17 (Low dependency) show the updated 2oo3 errors calculations using the Baseline Human Error Rate of 0.0041.



Event tree applies to Actions:
- Opening Sensor A/B/C root valve after maintenance
- Calibrating Sensor A/B/C
- Removing bypass from device A/B/C

Figure 16. Calculation of Conditional Probability of Failure in 2oo3 Actions
HEP: 0.0041 – High Dependency
Courtesy Process Improvement Institute, Inc., All Rights Reserved



Event tree applies to Actions:
- Opening Sensor A/B/C root valve after maintenance
- Calibrating Sensor A/B/C
- Removing bypass from device A/B/C

Figure 17. Calculation of Conditional Probability of Failure in 2oo3 Actions
HEP: 0.0041 – Low Dependency
Courtesy Process Improvement Institute, Inc., All Rights Reserved

Summary Table for this Example

Table 10 shows a summary of key parameters and results from the examples. The examples illustrate the effect of changes in the base human error probability for typical ways that human error can compromise an SIF. The table also shows some examples of error detection and correction that reduce the PFD.

As can be seen in Table 10, it is possible with enough extra effort to reduce human error or detect and recover from errors to be able to achieve a target PFD (even while accounting rigorously for human error probability) for a SIL 2 SIF. However, it is not quite possible to reach the target PFD for a SIL 3 SIF because there are limits to how far human error can be reduced.

Table 10. Summary table for SIL Calculations with Human Error calculations

						PFD for Human Errors								Detect and Recovery from Error				
Ex #	Figure	Baseline HEP	Target SIL	PDF Comp	Achieved SIL per 61511	Maint.	PFD Root Valves	PFD SIF Bypass	PFD Relay bypass	PFD Miscali	Total PFD SYS-HUM	Achieved PFD SIF per CCPS	Achieved SIL per CCPS	Detect & correct error	PFD Change	Total PFD SYS-HUM	Achieved PFD SIF per CCPS, Rev	Achieved SIL per CCPS, Rev
1	12	0.02	1	0.039	1		0.02	0.02		0.02	0.06	0.0990	🟩 1	Root valves	-0.0190	0.0410	0.0800	🟩 1
		0.04	1	0.039	1		0.04	0.04		0.04	0.12	0.1590	🟧 1	Root valves	-0.0380	0.0820	0.1210	🟧 1
1	13, 14, 15	0.02	2	0.008	2	No staggering	0.00522	0.02000	0.02000	0.00522	0.05044	0.05844	🟥 1	Root valves	-0.00496	0.04548	0.05348	🟥 1
	13, 14, 16	0.02	2	0.008	2	Staggering	0.00010	0.02000	0.02000	0.00010	0.04019	0.04819	🟥 1	SIF Bypass Relay bypass	-0.01900 -0.01900	0.00219	0.01019	🟧 2
2 high practice	13, 17, 18	0.0041	2	0.008	2	No staggering	0.00102	0.00410	0.00410	0.00102	0.01024	0.01824	🟧 1	Root valves	-0.00097	0.00927	0.01727	🟧 2
	13, 17, 19	0.0041	2	0.008	2	Staggering	0.00012	0.00410	0.00410	0.00012	0.00844	0.01644	🟧 2	SIF Bypass Relay bypass	-0.00390 -0.00390	0.00065	0.00865	🟩 2
3	NA	0.0041	3	0.0007	3	Staggering	0.00001	0.00410	0.00410	0.00001	0.00822	0.00892	🟥 2	SIF Bypass Relay bypass	-0.00390 -0.00390	0.00043	0.00113	🟧 **3**

Color legend:

🟩 Green	Meets the Target SIL PFD
🟧 Orange	Within the margin of error, meets the Target PFD, but does not comply with the strict criteria in IEC-61511 for achieving the Target SIL
🟥 Red	Misses the Target SIL by a significant amount; the actual SIL achieved is shown

Conclusion

The rules for LOPA should be strictly followed when claiming to use LOPA. However, other methods can be used to model human error probability, and these may result in a lower PFD than allowed with the rules of LOPA. But HRA methods typically will not allow a great reduction in the estimated PFD for the scenario. This observation was known to the inventors of LOPA, which is one of the reasons LOPA was invented (i.e., to simplify risk assessment). Further, rigorously accounting for human error that can occur during human interventions with SIF will make it very difficult to achieve a target PFD of 0.010 for SIL 2 SIFs and make it nearly impossible to achieve a target PFD of 0.0010 for SIL 3 SIFs.

Understanding and controlling accidents that are dominated by human error is still necessary, and only fully independent IPLs that can achieve their target PFD will allow achievement of the target mitigated event likelihood. **There is no substitute for having enough valid IPLs**.

Acronyms

APJ: Absolute Probability Judgment

BHEP: Base Human Error Probability

CCPS: Center for Chemical Process Safety

CSB: US Chemical Safety Board

COI: Consequence of Interest

DEMCO Valve: Isolation valve between reactor and a settling pipe from the polyethylene reactor

EPA: U.S. Environmental Protection Agency

HAZOP: Hazard and Operability study

HCR: Human Cognitive Reliability

HEART: Human Error Assessment and Reduction Technique

HEP: Human Error Probability

HRA: Human Reliability Analysis

HRET: Human Reliability Event Tree

IE: Initiating Event

IEF: Initiating Event Frequency

IPL: Independent Protection Layer

LOPA: Layer of Protection Analysis

LOTO: Lock Out Tag Out

OSHA: US Occupational Safety and Health Administration

PE: Polyethylene

PFD: Probability of Failure on Demand

PHA: Process Hazard Analysis

PII: Process Improvement Institute

PTO: Product Takeoff valve

PSM: Process Safety Management
PSV: Process Safety Valve
RBPS: Risk Based Process Safety
SIL: Safety Integrity Level
SLIM: Success Likelihood Method
SOP: Standard Operating Procedure
TaR: Time at Risk
THERP: Technique for Human Error Rate Prediction
UK HSE: United Kingdom Health and Safety Executive

References

[1] UK HSE, "RR679: Review of human reliability assessment methods," 2009.

[2] A. Swain and H. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (NUREG/CR-1278)," 1983.

[3] W. Bridges and G. Collazo, "Human Factors and Their Optimization," in *AIChE/CCPS 8th Global Congress on Process Safety*, Houston, 2012.

[4] US Chemical Safety and Hazard Investigation Board, "Investigation Report: Refinery Explosion and Fire, Report No. Report No. 2005-04-I-TX," 2007.

[5] D. Gertman, H. Blackman, J. Marble, J. Byers and C. Smith, *The SPAR-H Human Reliability Analysis Method (NUREG/CR-6883),* Washington DC: U.S. Nuclear Regulatory Commission, 2005.

[6] A. Swain, *Human Reliability Analysis Training Course,* ABS Consulting (formerly JBF Associates), 1993.

[7] US Federal Aviation Administration, *AC 120-42B - Extended Operations (ETOPS and Polar Operations),* Washington DC, 2008.

[8] W. Bridges, A. M. Dowell, H. Thomas and M. Massello, "SIL-3, SIL-2, and Unicorns (There Is a High Probability Your SIL 2 and SIL 3 SIFs Have No Better Performance Than SIL 1)," in *AIChE/CCPS 15th Global Congress on Process Safety*, New Orleans, 2019.

[9] W. Bridges and T. Clark, "LOPA and Human Reliability – Human Errors and Human IPLs (Updated)," in *AIChE/CCPS 7th Global Congress on Process Safety*, Chicago, 2011.

[10] W. Bridges, "LOPA and Human Reliability – Human Errors and Human IPLs," in *AIChE/CCPS 6th Global Congress on Process Safety*, San Antonio, 2010.

[11] R. Stack and P. Delanoy, "Evaluating Human Response to An Alarm for LOPA or Safety Studies," in *AIChE/CCPS 6th Global Congress on Process Safety*, San Antonio, 2010.

[12] J. Forester, *ATHEANA User's Guide (NUREG-1880),* Washington, DC: U.S. Nuclear Regulatory Commission, 2007.

[13] J. V. Bukowksi and W. M. Goble, "Analysis of Pressure Relief Valve Proof Test Data: Findings and Implications," in *AIChE 10th Plant Process Safety Symposium*, 2008.

[14] J. V. Bukowski and W. M. Goble, "Analysis of Pressure Relief Valve Proof Test Data," *AIChE Process Safety Progress,* 2009.

[15] J. V. Bukowski, "Results of Statistical Analysis of Pressure Relief Valve Proof Test Data Designed to Validate a Mechanical Parts Failure Database," Technical report, exida, 2007.

[16] CCPS/AIChE, Guidelines for Independent Protection Layers and Initiating Events in Layer, Wiley, 2012.